UNIVERSITY OF KWAZULU-NATAL

Cybersecurity for Industrial Internet of Things: a case study of the South African transport sector

By

Barend Hendrik Pretorius

Student Number: 200276341

A thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy in Information Systems

School of Management, Information Technology and Governance

College of Law and Management Studies

Supervisor: Prof Brett van Niekerk

Co-supervisor: Dr Karunagaran Naidoo

2024

Declaration

I, Barend Pretorius, declare that: -

i. The research reported in this thesis, except where otherwise indicated, is my original research;
ii. This thesis has not been submitted for any degree or examination at any other university;
iii. This thesis does not contain other persons' writing unless specifically acknowledged as being sourced from other persons;
iv. This thesis does not contain text, graphics or tables copied and pasted from the internet unless specifically acknowledged and the source being detailed in the thesis and in the reference section.

Barend Pretorius

(Student Number: 200276341)

Acknowledgements

Eerbewys en glorie aan die belangrikste, God. Vir my vrou, Elserie, my dogtertjies Amelia en Suné, en my ouers, Dr Buks en Charlotte Pretorius, wat my bygestaan het gedurende hierdie tyd, die skripsie is opgedra aan julle. Vir die res van my familie en vriende, baie dankie vir al julle ondersteuning.

To my supervisors, Prof Brett van Niekerk and Dr Karna Naidoo, your direction, proficiency and nurturing during this Doctoral journey are greatly appreciated. You are a continuous source of energy and inspiration for my academic career. You both have gone beyond the call of duty. Prof van Niekerk, you have consistently guided and supported me, without which I would not have completed this research. My colleagues and friends who participated or supported me with my research, thank you, it is much appreciated.

Abstract

There is an increasing drive for the fourth industrial revolution, which has resulted in increasing deployments of Industrial Internet of Things (IIoT). IIoT deployments have led to multiple security incidents. This study focuses on determining the factors influencing cybersecurity for IIoT and the pressing need to secure IIoT devices and networks in South Africa's transportation sector, which is crucial to the nation's economy. Examples include maritime, ports, railways, airports, trains, and road transportation.

A mixed-method approach is used. Quantitative methods include questionnaires, and qualitative methods include the analysis of documents (industry best practices, standards, and frameworks) used to identify and assess the technological, organisational, procedural and people factors influencing cybersecurity for IIoT in the transport sector of South Africa (SA). The population for this study consisted of 58 participants with knowledge of IIoT security in the transport sector of SA. Questionnaires are analysed using descriptive statistics, correlation, and inferential statistics. Data collected from documents are analysed using thematic analysis. The conceptual research framework underpinning this study is the Design Science Research combined with Business Model for Information Security (BMIS) framework. The areas of BMIS that guided the study are technology, organisation, procedure, and people.

The findings of this study bring to light significant organisational and procedural challenges, including the crucial role of cybersecurity staff for IIoT, the necessity for robust incident response plans, and the looming technological threats such as ransomware and cyber espionage. From a people factor, the lack of training, communication, and employee satisfaction emerges as a significant concern, underscoring the need for immediate attention and action.

Through the data triangulation from the qualitative and quantitative methods, the relationship between the four BMIS factors is determined, and a framework for IIoT cybersecurity in the SA transport sector is developed. The cybersecurity framework is evaluated against the MITRE ATT&CK framework.

Future research includes exploring control breakdowns, implementation feasibility, use of a honeypot to simulate IIoT device vulnerabilities, and alignment with legal requirements, thereby offering the potential for enhanced security measures for organisations in the South African transport sector.

Contents

List of Figures

List of Tables

List of Acronyms

ANC	African National Congress
AMQP	Advanced Message Queuing Protocol
BAN	Body Area Network
BCP	Business Continuity Plan
BLE	Bluetooth and Bluetooth Low-Energy
BMIS	Business Model for Information Security
CAC	Cybercrimes and Cybersecurity Bill
CAN	Campus/Corporate Area Network
CCTA	Central Computer and Telecommunications Agency
CCTV	Closed-Circuit Television
CIA	Confidentiality (C), Integrity (I) and Availability (A)
CD	Compact Disk
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CIP	Critical Infrastructure Protection
CMDB	Configuration Management Database
CMM	Capability Maturity Model
CoAP	Constrained Application Protocol
COBIT	Control Objectives for Information and Related Technology
CPI	Common Industrial Protocol

CPNI	Centre for the Protection of National Infrastructure
DBSA	Development Bank of Southern Africa
D2D	Device-to-device
DCE	Data Communication Equipment
DCPS	Data-Centric Publish-Subscribe
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service
DDS	Data Distribution Service
DHCP	Dynamic Host Control Protocol
DLRL	Data-Local Reconstruction Layer
DNP3	Distributed Network Protocol
DNS	Domain Name Servers
DoS	Denial of service
DRP	Disaster Recovery Plan
DSR	Design Science Research
DTE	Data Terminal Equipment
DVD	Digital Video Disc
ECT	Electronic Communications and Transactions
ENISA	European Union Agency for Network and Information Security
FBI	Federal Bureau of Investigation
GCIS	Government Communications and Information Services
GE	General Electric
HVAC	Heating, Ventilation, and Air-Conditioning
HMI	Human Machine Interface

HR	Human Resources
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICCP	Inter Control Center Protocol
ICCWS	International Conference on Cyber Warfare and Security
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
ID	Identity Document
IEC	International Electrotechnical Commission
IED	Intelligent electronic device
IJCWT	International Journal of Cyber Warfare and Terrorism
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IOL	Independent Online
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardisation
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITS	Intelligent Transportation Systems
KPI	Key Performance Indicators
LAN	Local area network
MAN	Metropolitan Area Network
MISS	Minimum Information Security Standard

MQTT	Message Queue Telemetry Transport
MTU	Master Terminal Unit
NASA	National Aeronautics and Space Administration
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NFC	Near-Field Communication (NFC) -
NGO	Non-Governmental Organisation
NPO	Non-profit Organisation
OT	Operational Technology
PAN	Personal Area Network
PIN	Personal Identification Number
PLC	Programmable Logic Controllers
POPI	Protection of Personal Information
RFID	Radio Frequency Identification
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information
RTMC	Road Traffic Management Corporation
RTU	Remote Terminal Unit
SA	South Africa
SABC	South African Broadcasting Corporation
SAIEE	South African Institute of Electrical Engineers
SANRAL	South African National Road
SANS	System Administration, Audit, Network and Security
SCADA	Supervisory Control and Data Acquisition

SIC	Security Intelligence Centre
SIEM	Security Information and Event Management
SIS	Safety Instrumented Systems
SOC	State-Owned Company
SQL	Structured query language
TCP	Transport Communication Protocol
TTP	Tactics, Techniques, and Procedures
USB	Universal Serial Bus
UK	United Kingdom
VPN	Virtual Private Network
WAN	Wide Area Network

Chapter 1 Introduction

1.1 Introduction

The Internet of Things (IoT) is taking off exponentially as the world embraces the fourth industrial revolution. More devices, things and gadgets are connected to the internet. It is predicted that there will be over 30 billion IoT-connected devices by 2025 (Weston, 2023).

Most of these devices are intended for consumers. Businesses and industries are already exploring the possibilities and capabilities of IoT devices to gain a competitive advantage in their respective sectors. IIoT (Industrial Internet of Things) refers to IoT devices that monitor and control industrial and related processes such as energy, healthcare, retail, smart manufacturing, intelligent transport, and operations. With the integration of IIoT into business processes, there are increased risks due to convergence with cloud computing, mobile, and other platforms. This not only complicates the design but also introduces more risks.

Several cybersecurity incidents associate with IoT and IIoT devices worldwide. As the deployment of IoT devices continues without security considerations, the prevalence of DDoS attacks utilising these devices is expected to rise. In October 2016, the most significant cyberattack brought down half of America's internet using compromised connected devices (Woolf, 2016). The DDoS attack was initiated using IoT devices. These IoT devices were infected with malware known as Mirai botnet and blasted Dyn, which controlled the Domain Name Servers (DNS), taking most internet websites offline.

Johnson, via Gartner (Johnson, 2023), indicated a lack of awareness and knowledge concerning best practices for IoT security, highlighting a need for a holistic and comprehensive approach to ensure the security of devices, communication infrastructure, and applications in the IoT environment.

International professional bodies have developed IoT and IIoT cybersecurity frameworks as listed in Section 2.3.8. Furthermore, it remains uncertain whether the frameworks sufficiently cover the risks, threats, and vulnerabilities specific to the transport sector of South Africa (SA), discussed in Section 2.3.10, necessitating a more thorough evaluation. This research used a mixed methods approach to determine the technological, organisational, procedural and people factors influencing IIoT cybersecurity in the SA transport sector and, through the investigations, developed a cybersecurity framework aligned to South African legislation. Figure 1.1 is a graphical representation of the outline of this chapter and its overall structure.

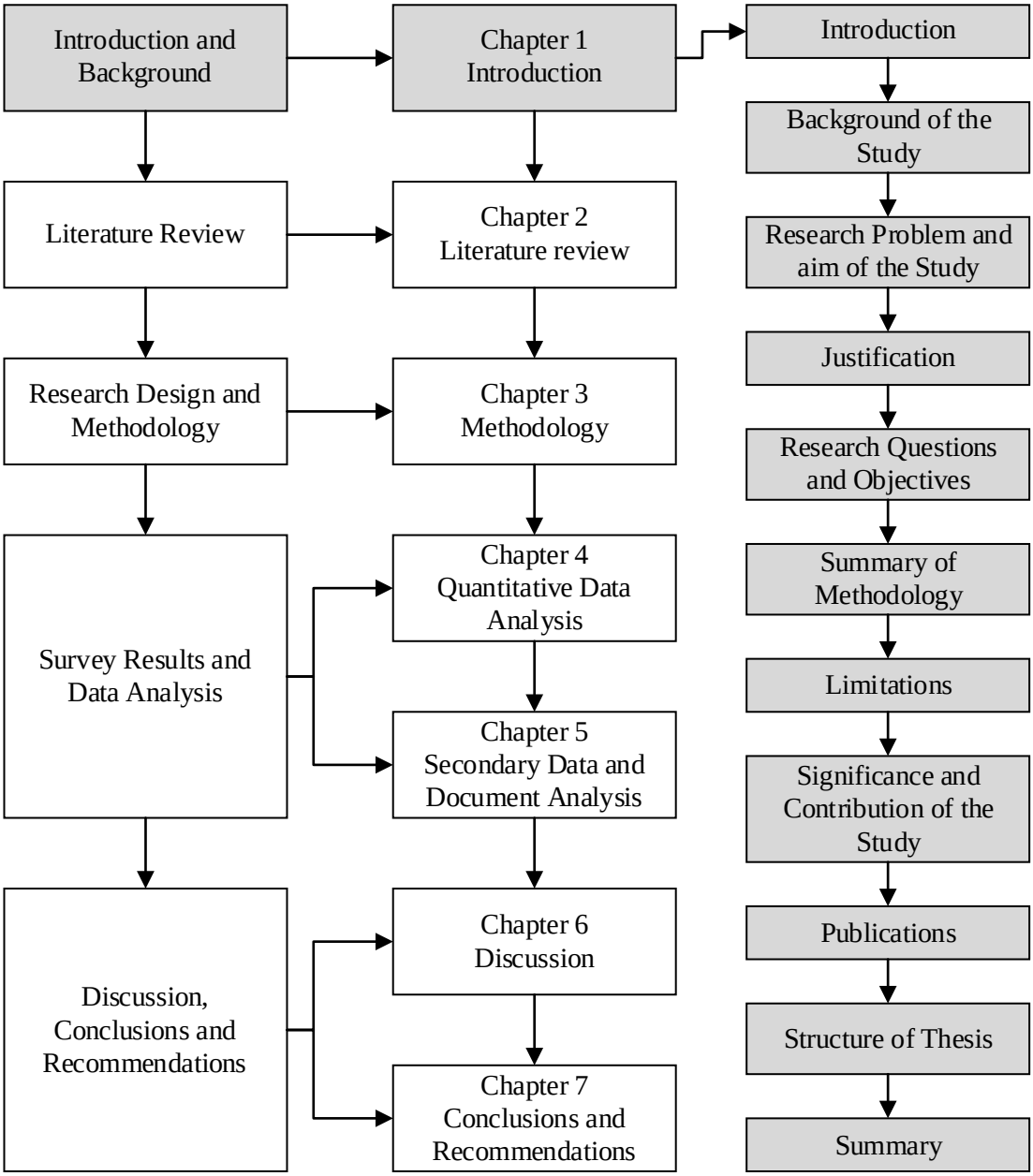
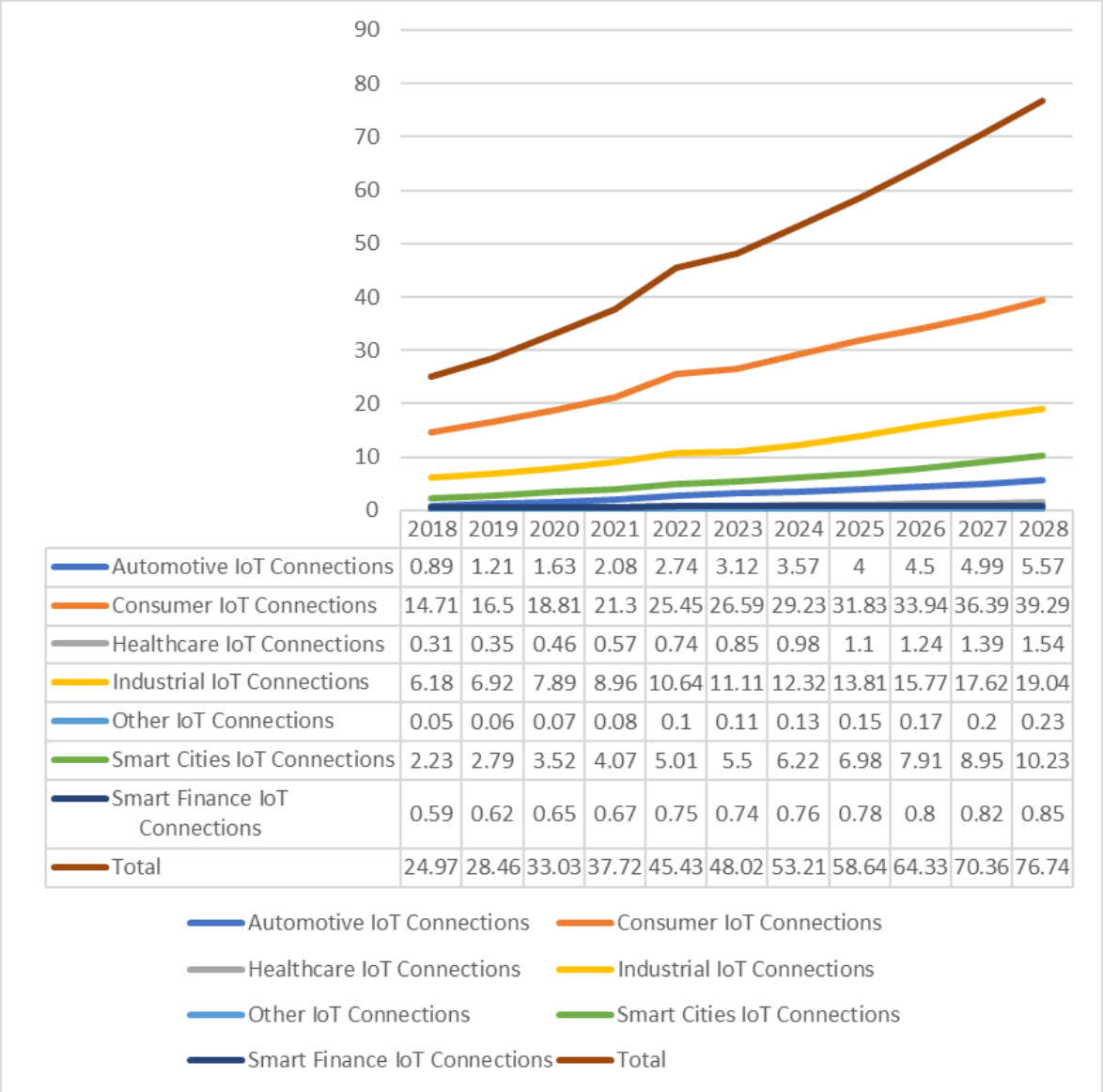


Figure 1-1: Graphical representation of Chapter 1 outline

1.2 Background of the Study

According to the latest Global Cybersecurity Index published by the International Telecommunication Union (ITU) (ITU Publications, 2024), SA has been ranked 59th out of 182 countries in terms of its commitment to cybersecurity. This suggests that a significant amount of work needs to be done to secure the country's cyberspace effectively. This gap might increase further with the deployment of IoT and IIoT. There is an increase in IoT implementation as local companies IoT.nxt and SqwidNet invest in IoT. IoT.nxt has raised R100 million for expansion (Venktess, 2017), and SqwidNet implemented an ultra-narrow band network at a low cost (Mybroadband, 2017). Transnet and General Electric (GE) have collaborated to bring IIoT to Africa and digitise the transport sector (CNBC Africa,

2017). According to Engineering News (Burger, 2021), IoT vehicle applications gained popularity among South African consumers. Meanwhile, municipalities are adopting IoT to improve public sector transportation. Examples of the IIoT deployments are discussed in Section 2.4.9. IoT deployment in SA is predicted to grow by 14% yearly between 2020 and 2025. As of March 2024, South Africa's growth rate of 13.6% is slightly lower than the expected 14%. However, it is projected to reach $11.3 billion by 2028 (iONLINE, 2023). Figure 1.2 shows the historical and predicated growth rates, in millions, as of March 2024, for IoT deployments (including IIoT) in the South African market (Statista, 2024).



	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Automotive IoT Connections	0.89	1.21	1.63	2.08	2.74	3.12	3.57	4	4.5	4.99	5.57
Consumer IoT Connections	14.71	16.5	18.81	21.3	25.45	26.59	29.23	31.83	33.94	36.39	39.29
Healthcare IoT Connections	0.31	0.35	0.46	0.57	0.74	0.85	0.98	1.1	1.24	1.39	1.54
Industrial IoT Connections	6.18	6.92	7.89	8.96	10.64	11.11	12.32	13.81	15.77	17.62	19.04
Other IoT Connections	0.05	0.06	0.07	0.08	0.1	0.11	0.13	0.15	0.17	0.2	0.23
Smart Cities IoT Connections	2.23	2.79	3.52	4.07	5.01	5.5	6.22	6.98	7.91	8.95	10.23
Smart Finance IoT Connections	0.59	0.62	0.65	0.67	0.75	0.74	0.76	0.78	0.8	0.82	0.85
Total	24.97	28.46	33.03	37.72	45.43	48.02	53.21	58.64	64.33	70.36	76.74

Figure 1-2: IoT deployments (in million) in South Africa

Adopted from: Statista (2024)

As Mngadi (2021) pointed out, the fast implementation of IIoT without adequate cybersecurity measures could lead to significant risks. Mngadi (2021) also indicated that the rapid expansion of IoT

has led to increased sophistication in malicious software and the development of deceptive techniques for carrying out cyberattacks. According to Mngadi (2021), the development of security requirements is still nascent, highlighting a significant gap in addressing cybersecurity needs. Bertin and Mavoori (2022) argue that cybersecurity is often ignored due to its perception as a non-functional requirement for IoT and IIoT devices, further emphasising the need for immediate action. IT News Africa (2018) mentioned the increasing importance of security in the future of the Industrial Internet of Things (IIoT).

There exist control frameworks and standards internationally for IIoT and IoT. Baker (2021) states that not all IoT cybersecurity management frameworks adequately address cybersecurity-related risks. Furthermore, these international frameworks and standards might not be aligned with South African legislation. There is new legislation in South Africa, including the Cybercrimes Act (Government of Republic of South Africa, 2020) and the Protection of Personal Information (POPI) Act (Government of Republic of South Africa, 2013). Existing legislation include Electronic Communications and Transmissions (ETC) Act (Government of Republic of South Africa, 2002a), the Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) Act (Government of Republic of South Africa, 2002b), and King IV (Institute of Directors in Southern Africa, 2009). IIoT and IoT implementation in SA is growing; however, SA needs to catch up to the rest of the world regarding their cybersecurity commitment as indicated by the Global Cybersecurity Index (ITU Publications, 2024). Consequently, securing IIoT and IoT devices monitoring key business processes is necessary. These processes are critical to the South African economy and businesses implementing these. No previous study or current cybersecurity framework is considering IIoT deployment in the transport sector in SA.

1.3 Research Problem and Aim of Study

The current state of IIoT in SA and the factors influencing IIoT security were unknown as there are limited studies and research in this area. These include the technological, organisational, procedural and people factors influencing the cybersecurity of IIoT in the transport sector of SA. This research gained an understanding of the unique factors in the sector by identifying and assessing the degree of relationships among the factors influencing IIoT cybersecurity in SA's transportation sector. Based on input from experts in the sector and best practices, a cybersecurity framework aligned to the transport sector of SA was developed and validated.

1.4 Justification

There is an increasing drive for the fourth industrial revolution resulting in deployments of IIoT across various sectors. The current state of IIoT in the transportation sector of SA and the factors influencing

IIoT are not fully understood, as there are no previous studies and research in this area as illustrated in Section 1.9. Although there are some studies internationally, nothing exists in this area locally.

Cybersecurity risk is listed as the number two business risk in SA for 2023, according to the global Allianz report (Allianz Global Corporate & Specialty, 2023).

As discussed in Section 1.2, IT News Africa (2018) emphasized the growing significance of security in shaping the future landscape of IIoT. This observation underscores the evolving challenges and considerations of safeguarding IIoT ecosystems against potential threats and vulnerabilities. It also highlights security as a top trend and emphasises the need for robust security measures in IIoT deployments. As IIoT devices and networks become more interconnected and integrated into critical infrastructure, they become potential cyberattack targets. It emphasises the significance of protecting IIoT systems from threats like unauthorised access, data breaches, and disruption of operations. Security should be built into the design and implementation of IIoT systems from the beginning (IT News Africa, 2018).

According to Coldewey (2019), 90% of IoT devices are manufactured without considering security. The United Kingdom (UK) does have a security code of practice for IoT (Government of UK, 2018). SA has recently finalised the Cybercrimes Act (Government of Republic of South Africa, 2020), which does not include IoT or IIoT cybersecurity. There is no SA legislation like the UK which included IoT or IIoT and security thereof.

As indicated by the Global Cybersecurity Index (ITU Publications, 2024), SA's efforts towards cybersecurity are also behind while pushing ahead with the fourth industrial revolution. Given the increasing incidents of IIoT worldwide and in the transport sector, it is of utmost importance to anticipate and mitigate these emerging and disruptive technologies for the future. The notable increase in cyberattacks within the transportation sector indicates that organisations incorporate new technologies (such as IIoT) without enhancing their security protocols. This underscores the vulnerability of even traditional sectors to cyber threats when there is a shift in the technological landscape. Organisations must recognise that any technological upgrade should be accompanied by a thorough reassessment of cyber risks (Penta Security, 2023).

IIoT cybersecurity is still growing in SA and has not yet been fully established. As mentioned in Section 1.3, this study intents to fill a gap of limited academic studies done in the South African context.

The transportation sector was selected as the study area based on its pivotal role in facilitating the movement of individuals, commodities, and finances. It is widely acknowledged that the transportation sector plays an essential role in the functioning of modern societies, and therefore, it

was deemed a suitable subject of investigation. Given its indispensable function in local and global commerce and monetary transactions, the transportation industry is increasingly becoming a prime target for cyber adversaries (Penta Security, 2023). According to the Development Bank of South Africa (DBSA, n.d.), the transportation industry in SA plays a pivotal role in fostering socio-economic development and promoting growth on a global scale. It constitutes a fundamental element in South Africa's competitiveness within international markets.

As demonstrated in Section 2.3.6, there has been a surge in cyberattacks targeting various modes of transportation, including aviation, maritime, railways, and roads.

Naval Dome, an Israeli cybersecurity specialist, has reported a 400% increase in attempted hacks over the last six months, beginning in February 2020. This surge in cyberattacks is directly linked to the maritime industry's adoption of new technology (Security Magazine, 2020). The severity of the situation is further highlighted by the fact that all four major container shipping companies, Maersk, CMA CGM, MSC, and Cosco Shipping, have fallen victim to cyberattacks (Booth, 2021).

Transportation is vulnerable to cyberattacks, causing widespread damage. They have the potential to disrupt or even halt entire systems and services, such as transport booking platforms for airlines and railways. They can also lead to the exposure or obstruction of access to sensitive data, compromising the safety of both staff and passengers, and have ripple effects severely impacting supply chains (CyberPeace Institute, n.d.). The 2021 cyberattack on Transnet in South Africa, as discussed in Section 2.4.6.2, is a stark example of these potential disruptions, leading to significant economic consequences.

Shortly following Transnet's restoration to full operational capacity post-cyberattack, significant delays arose within the supply chain. Warehousing and cold storage facilities were notably affected, resulting in products facing the risk of spoilage and animal feed being delayed at the Durban port (Smith, 2021). The scenario represented a "perfect storm" situation that had the potential to result in food shortages across South Africa, which prompted urgent calls for government intervention by two organisations: the SA Meat Processors Association and the SA Association of Meat Importers and Exporters (TimesLIVE, 2021).

This study commenced in mid-2017 and already identified the need to investigate and strengthen the transport sector's cybersecurity. This was two years prior to the massive attack on Transnet, which further confirmed the need.

This study assesses the current state of IIoT cybersecurity in the transportation sector of SA, given the critical role transportation play in the South African economy and the increase of cyberattacks in this sector as demonstrated in Section 2.4.7, and develop an IIoT cybersecurity framework to address

common concerns by taking into account new and existing legislation. This IIoT cybersecurity framework will enable organisations in the transportation sector of SA to improve the cybersecurity of their IIoT systems, leading to greater availability and reliability of computer systems.

1.5 Research Questions and Objectives

The main objective of this study is to identify and assess the factors and the degree of relationships among the factors influencing IIoT cybersecurity in the transport sector of SA to develop and validate a cybersecurity framework aligned with the SA transport sector.

The research aims are broken down into the following research questions and objectives.

1.5.1 Research Questions

The research questions underpinning this study are:

1. What are the technological factors influencing IIoT cybersecurity of the SA transport sector?
2. What are the organisational factors influencing IIoT cybersecurity of the SA transport sector?
3. What are the procedural factors influencing IIoT cybersecurity of the SA transport sector?
4. What are the people factors influencing IIoT cybersecurity of the SA transport sector?
5. What is the degree of the relationships amongst the technological, organisational, procedural and people factors for IIoT cybersecurity of the SA transport sector?
6. How to develop and validate a cybersecurity framework for IIoT in the SA transport sector using the data collected?

1.5.2 Research Objectives

The objectives of this study are:

1. To determine the extent to which the technological factors influence IIoT cybersecurity of the SA transport sector:
    - Existing and new threats due to IIoT.
    - Vulnerabilities.
    - Risks.
2. To critically assess the organisational factors influencing IIoT cybersecurity of the SA transport sector:
    - Size and structure.
    - Cybersecurity strategy.
    - Risk appetite.
    - Innovativeness culture.

- Security culture.
- Senior executive engagement with security.

3. To critically assess the procedural factors influencing IIoT cybersecurity of the SA transport sector:
    - Security incident response.
    - Risk management.
    - IT governance and compliance.
    - Policies, standards, and procedures.
    - Legal and regulatory requirements.
4. To critically assess the people factors influencing IIoT cybersecurity of the SA transport sector:
    - Cybersecurity awareness.
    - Enablement.
    - Employee engagement.
    - Employee satisfaction.
5. To assess the degree of the relationships amongst the BMIS factors for IIoT cybersecurity in the SA transport sector.
6. To develop and validate a cybersecurity framework for IIoT in the SA transport sector using the data collected.

1.6 Summary of Methodology

Design Science Research is used for the process of designing the control framework. Design Science Research (DSR) is combined with the Business Model for Information Security (BMIS) to form the conceptual framework to guide the study. The research tools underpin a mixed methods approach: quantitative instruments include questionnaires; qualitative tools include document analysis.

A cross-sectional study is done to determine the state of IIoT in the transport sector of SA at a single point in time. Due to limited available information on individuals with experience with IIoT and security in the sector, non-probabilistic sampling is appropriate, and convenience sampling is used and enhanced with snowball sampling. The questionnaire's sample size is at least 30 people from various professional organisations utilising IIoT systems; these include Information Systems Audit and Control Association (ISACA), CISO Alliance and a large State-Owned Company (SOC). Data collected from questionnaires are analysed using Excel (with statistical plugins). Documents in the form of cybersecurity standards, frameworks and best practices are selected based on their IIoT

relevance and relevance to the responses from the questionnaires. The documents are analysed, coded, and summarised through thematic and content analysis using the software NVivo.

1.7 Limitations

It is difficult to determine the exact population as there are no studies on the cybersecurity of IIoT in the SA transport sector conducted and challenging to determine the individuals with IIoT security knowledge. An online questionnaire was distributed to organisations in the transportation sector and through professional bodies to solicit responses (refer to Section 1.6), and a question is included upfront to determine the relevance of the respondents. This is a case study of the SA transportation sector; the methodology can be applied to other countries and sectors as a starting point to develop a relevant control framework; however, the relevant legal and regulatory requirements for that country must be considered.

1.8 Significance and Contribution of the Study

The study provides a unique South African viewpoint. As noted in Section 1.2, the importance of cybersecurity for IoT and IIoT devices is sometimes overlooked, as it is often viewed as a non-functional requirement (Bertin & Mavoori, 2022). However, with the projected rapid expansion of IoT and IIoT both globally and in SA (iONLINE, 2023), this disregard for cybersecurity could pose a significant risk. As mentioned in Section 2.4, limited academic studies are done in South Africa, which contributes by providing this knowledge, therefore, this study fills this gap.

The main contribution of this study is a prioritised cybersecurity control framework, which has been derived based on input provided by experts in the transport sector and by combining the best practices. This was constructed from the technological, organisational, procedural, and people factors influencing IIoT in the transport sector of South Africa as determined by the study.

New methodologies are also introduced, first combining design science with BMIS, and then using MITRE ATT&CK framework for ICS in design science to validate the cybersecurity framework. Multiple publications and contributions to industry emerged from this study; refer to Section 1.9.

1.8.1 Contribution to Theory

This study created a conceptual model combining the BMIS framework and Design Science Research to aid in developing a cybersecurity framework for IIoT in the transportation sector. The benefit of the model is that it considers various BMIS factors, including technological (threats, vulnerabilities, and risks) and organisational, procedural, and people-related factors, to develop a cybersecurity framework relevant to South Africa's transportation sector. For future work or research, the feasibility and effectiveness of the cybersecurity framework in the transport sector need to be evaluated.

Another contribution is using MITRE ATT&CK framework for ICS as part of Design Science Research to validate the cybersecurity framework. The advantage of validating the cybersecurity framework against the MITRE ATT&CK framework is that it verifies its effectiveness through real-world adversary tactics used by cybercriminals and hackers in real-world scenarios. This contribution developed a model allowing future researchers to verify and validate their IIoT cybersecurity frameworks against the MITRE ATT&CK framework.

1.8.2 Contribution to Global Knowledge

IIoT is a growing area, and since limited research into cybersecurity has been conducted for the transportation sector, there is knowledge sharing because of the study. Parts of the literature on IoT and IIoT, including the incidents, threat, vulnerabilities and risks from this study, was published as an academic journal in the *Journal of Information Warfare* in 2020 (Pretorius & Van Niekerk, 2020) and the Proceedings of the *14th International Conference on Cyber Warfare and Security* (ICCWS) on in March 2019 (Pretorius & Van Niekerk, 2019). Parts of the literature on IIoT and incidents and the research from the primary data on threats, vulnerabilities, and risks were published in the Journal *Scientia Militaria* in 2023 (Pretorius & Van Niekerk, 2023).

1.8.3 Contribution to Practice

The current state of IIoT in SA and the factors influencing IIoT are assessed as these are unknown. There are limited studies and research in this area. The technological, organisational, and environmental factors influencing the security of IIoT in the SA transportation sector are unknown. This research identified the factors, assessed the degree of relationships among the factors influencing IIoT cybersecurity, and developed a cybersecurity framework aligned with South African regulations. The cybersecurity control framework benefits organisations by identifying factors influencing IIoT deployment and helping implement controls to mitigate the threats, risks, and vulnerabilities to secure the IIoT devices in their environments.

Aspects of this study were presented at a practitioner conference, namely at the annual IT Web Security Summit in July 2020, at an academic conference, the 14th International Conference on Cyber Warfare and Security (ICCWS) in March 2019, and as two invited presentations to the South African Institute of Electrical Engineers (SAIEE) in March 2019 and CISO Alliance Durban Chapter in July 2019.

1.9 Publications

This is a Doctoral thesis; however, the following publications and presentations emanated from the research:

- **Academic conference:** Pretorius, B., & Van Niekerk, B. (2019). IIoT Security: Do I really need a Firewall for my Train? *The Proceeding of the 14th International Conference on Cyber Warfare and Security* (pp. 338-347). UK: Academic Conferences and Publishing International Limited.
- **Invited presentation:** Pretorius, B. (2019). Industrial Internet of Things (IIoT) Security *South African Institute of Electrical Engineers (SAIEE) March 2019*.
- **Invited presentation:** Pretorius, B. (2019). Industrial Internet of Things (IIoT) Security *CISO Alliance Durban Chapter July 2019.*
- **Academic journal:** Pretorius, B., & Van Niekerk, B. (2020). Industrial Internet of Things Security for the Transportation Infrastructure. *Journal of Information Warfare, 19*(3), 50-67. Retrieved from https://www.jstor.org/stable/27033632.
- **Invited presentation:** Pretorius, B., & Van Niekerk, B., 2020, 'IOT security: Do I need a firewall for my light bulb?' *IT Web Security Summit 2020.*
- **Academic journal:** Pretorius, B., & van Niekerk, B. (2023). IoT and IIoT Security for the South African Maritime and Freight Transportation Sectors, *Scientia Militaria*

Related publication not directly emanating from the thesis:

- **Book Chapter:** Van Niekerk, B., Pretorius, B., Ramluckan, T., & Patrick, H. (2018). The Impact of IoT on Information Warfare, Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution, pp 141-164, IGI Global.

1.10 Structure of the Thesis

The thesis comprises a total of seven chapters, which includes the present chapter. This chapter introduced the study and described the research approach. Chapter 2 presented a literature review on IIoT. Chapter 3 discussed the research methodology, research design and conceptual framework that guided this study. Chapter 4 presented the quantitative data analysis, while Chapter 5 looked at various documents (cybersecurity frameworks) that are qualitatively analysed. Chapter 6 presented a discussion based on the data analysed, the impact to the transportation sector and the cybersecurity framework development and validation. Chapter 7 concludes the study by presenting the findings, discussing limitations, suggesting areas for future research, and offering a summary.

1.11 Summary

IIoT is an umbrella term that refers to the use of IoT devices in monitoring and controlling industrial and related processes. The IIoT encompasses a wide range of fields, including intelligent transport. As the IIoT becomes more intertwined with business operations, it intergrades with cloud computing,

mobile, and other platforms. While this integration can enhance performance and productivity, it also introduces greater complexity into the design process and increases risk.

Several cybersecurity incidents relate to IIoT and IoT worldwide. The DDoS attacks using IoT devices continue to increase as more IoT devices are deployed without any security considerations.

The current state of IIoT in the South African transport sector and the factors influencing IIoT security are not known as there limited studies and research in this area. These include the technological, organisational, procedural and people factors influencing the cybersecurity of IIoT in the transport sector of SA. This research identified and assessed the degree of relationships amongst the factors influencing IIoT cybersecurity in the transport sector of SA to develop and validate a cybersecurity framework aligned with the SA transport sector.

Chapter 2 Literature Review

2.1 Introduction

This chapter briefly introduces information security, incidents, and controls. Then introduce ICS/SCADA, IoT and IIoT environments, their components, and a comparison between IoT, IIoT and ICS/SCADA. International IIoT incidents and vulnerabilities, and threats are discussed. The background of the research objectives, namely IIoT in the SA transport sector, and legislation and challenges are discussed. The next chapter explores this methodology and the study's research methodology in more detail. Figure 2.1 is a graphical representation of the outline of this chapter and its overall structure.

IoT is taking off exponentially as the world approaches the 4th industrial revolution (Burkhalter, 2022b; Kumar, Tiwari, & Zymbler, 2019; World Economic Forum, 2016). More devices, things and gadgets are connected to the internet. Gartner (2017) forecasted that by 2020 there would be 20 billion IoT and IIoT devices joined to the internet. However, statistics indicated there were 16.4 billion IoT devices in 2022, a lesser growth than expected mainly due to the Covid pandemic. The new prediction is that there will be over 30 billion IoT-connected devices by 2025 (Weston, 2023).

Most of these devices are intended for consumers. Nevertheless, businesses and industries are actively investigating the potential and functionalities of IoT devices within their specific sectors to achieve a competitive edge. Consumer IoT devices include smart wearables, smart homes, appliances, cars, etc. IIoT refers to IoT devices designed to oversee and manage industrial processes. More risks are introduced as IIoT integrates with cloud computing, mobile and other platforms.

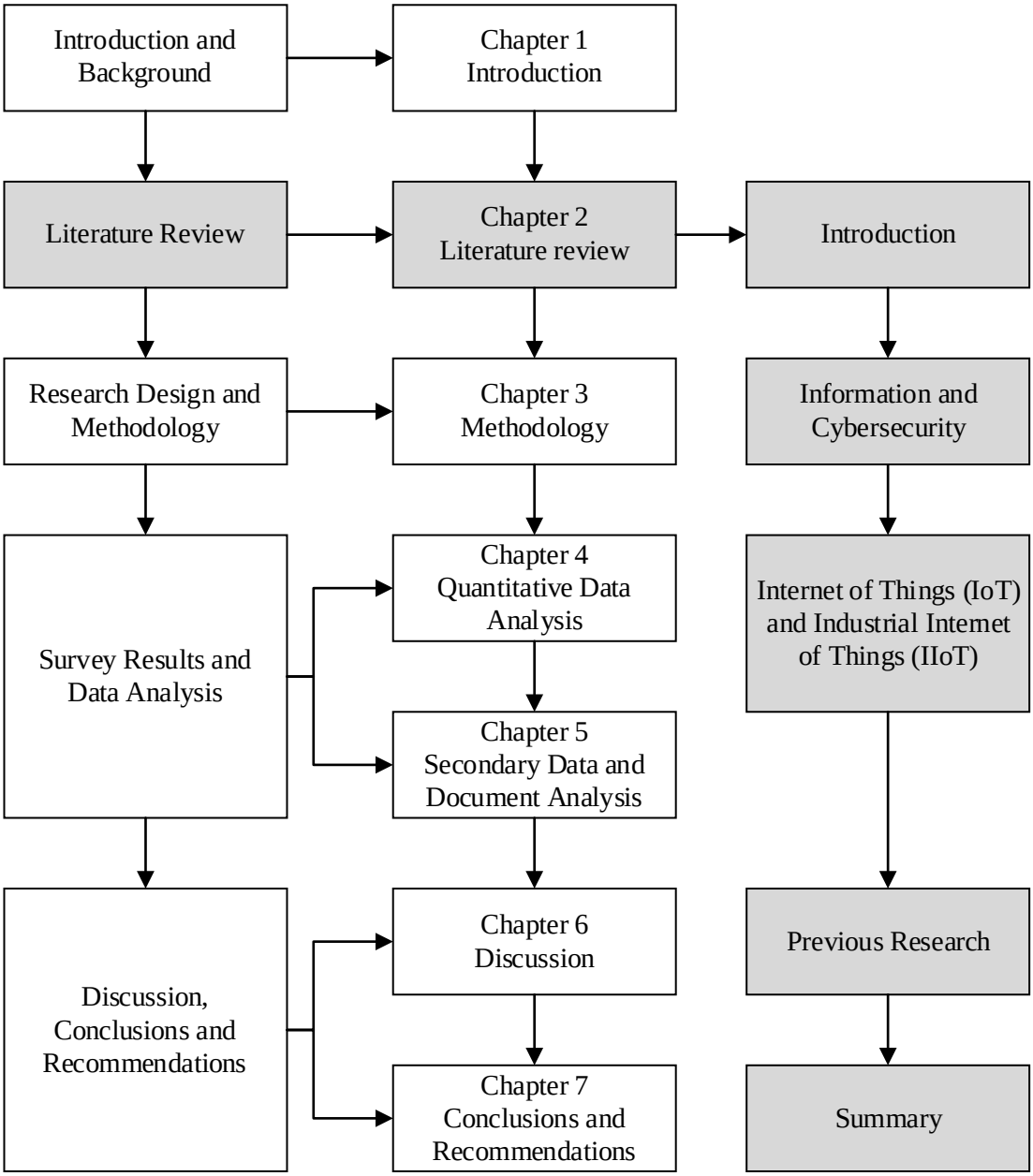


Figure 2-1: Graphical representation of Chapter 2 outline

2.2 Information and Cybersecurity

According to Whitman and Mattord (2012), security means being protected from potential risks or dangers. This protects a company's information assets from unauthorised access, alteration, examination, recording, leakage, disruption, or destruction in any form or circumstance. The essence of information security lies in safeguarding these valuable assets, fortifying intangible assets, optimising business processes, and instilling stakeholder confidence (Susanto, Almunawar, & Tuan, 2012). Critical components such as systems, hardware, storage, information transportation, individuals, and associated processes must be addressed by implementing policies, procedures,

awareness initiatives, user training, and using information security tools and technologies (Whitman & Mattord, 2012, p. 10).

Information security is not a one-time task or the responsibility of a single department. It requires a comprehensive approach covering every company aspect (RSA, 2014). This approach involves continuous monitoring, detection of abnormal events, and prompt response to threats (Esri, 2014, p. 2). Securing a company's information assets is a team effort that requires the collaboration of various roles (Carroll, 2014, p. 12). Each role has a unique contribution, highlighting the importance of collective effort).

Table 2-1: Categories to secure a company's information assets (Carroll, 2014)

Categories	Description
Physical security and environmental controls	Procedures to protect an organisation's assets and people from threats, including unauthorised physical access or natural disasters.
Operations security	Procedures to ensure the organisation can perform its operations with limited interruptions or compromises. This includes the capability to prevent, detect, respond, and recover when an incident or compromise occur such that normal operations can continue.
Communications security	This includes the protection of the organisation's transport of data and media with supporting tools to enable its objectives.
Network security	Protecting and monitoring an organisation's networks and devices to ensure it is used according to their purpose without compromise or downtime.
Database security	Protection of an organisation's data stored in a database
Storage security	Expert techniques to protect an organisation's information in its storage area networks (Whitman & Mattord, 2012, p. 8).

According to (Whitman & Mattord, 2012, pp. 29-33), Information Security Governance is agreed-upon roles and responsibilities implemented by the board and executive management to align information security with business strategy, ensuring the attainment of objectives while mitigating and managing risks and threats to information resources.

2.2.1 Information Security Triad

Information Security relies on the fundamental principles outlined in the "CIA Model" or "CIA triangle," as elucidated by Whitman and Mattord (2012:11-13). This model delineates three core aspects essential for safeguarding information: Confidentiality (C), integrity (I), and availability (A).

Confidentiality pertains to controlling access to sensitive information, confirming that only authorised individuals can access it, while unauthorised access constitutes a breach (Whitman & Mattord, 2012, pp. 11-13).

Integrity concerns the reliability and completeness of information, necessitating that it remains uncorrupted and undamaged; any compromise to this integrity signifies a breach (Whitman & Mattord, 2012, pp. 11-13).

Availability refers to the timely accessibility of information and infrastructure to authorised users, with any disruption or unavailability constituting a compromise (Whitman & Mattord, 2012, pp. 11-13).

These CIA principles are crucial considerations in the design, construction, and enhancement of secure systems, with their relative importance varying depending on the information system's nature. For instance, operational systems prioritise availability over confidentiality, whereas financial systems prioritise confidentiality and integrity over availability (Shilenge & Telukdarie, 2021).

It is also essential to ensure non-repudiation mechanisms, which prevent users from denying their actions. Examples include digitally signing emails or documents.

2.2.2 Vulnerabilities, Threats, Incidents and Risks

To ensure a successful information security strategy, organisations must identify and mitigate risks, threats, and vulnerabilities (Rhodes-Ousley, 2013). The definitions are listed in Table 2.2.

Table 2-2: Definition of vulnerability, threat, incident, and risk

Concept	Definition
Vulnerability	A vulnerability is a fault in a software program or program code that allows unauthorised modification or destruction of data or a single point of failure or misconfiguration, which could result in the CIA (discussed in Section 2.2.1) of information being compromised (Shahriar & Zulkcernine, 2012).
Threat	Exploiting a weakness in a current vulnerability is known as a threat (Dahbur, Mohammad, & Tarakji, 2011, p. 3). This could cause damage to the data and systems. A vulnerability could be exploited to gain unauthorised access to a company's network, systems, and, ultimately, sensitive data (Dahbur et al., 2011).
Incident	An incident is defined by Jones (2013:8-9) as an event that could include: • Unauthorised access to an organisation's network and systems. • Unauthorised access to confidential information. • Virus/malware outbreak on an organisation's systems or network. • Unauthorised interruption or denial of access to an organisation's data or systems; and • Unauthorised or accidental destruction or altering of an organisation's data.
Risk	According to the SANS Institute (2006), the risk is the possible damage arising from a current or future process. SANS Institute (2012) also defines risk as the likelihood of a provided threat source exploiting a potential vulnerability and its impact on an organisation. The general definition used to calculate risk according to Boehm (1991) is: *Risk = Probability x Impact*

2.2.3 Information Security Controls

The adequate security of a company's information assets relies on the collaborative efforts of various categories, as outlined by Carroll (2014), including physical security, operations security, communications security, network security, database security, and storage security. These categories must work in tandem to ensure comprehensive protection against potential threats.

2.2.3.1 Monitoring

In contemporary network security practices, threat management is vital, as it daily employs advanced techniques such as network security correlation. This involves integrating and analysing data from various sources to discern relationships, patterns, and trends indicative of potential security threats. The Security Information and Event Management (SIEM), housed within a Security Intelligence Centre (SIC), is valuable in this endeavour. It can collect and aggregate pertinent data from multiple sources, including firewall logs, intrusion detection and prevention systems, network device data, and operating system or application logs (Amoroso, 2013).

2.2.3.2 Capability Maturity Model

According to Acohido (2015), organisations commonly utilise a Capability Maturity Model (CMM) as a framework to assess their information security maturity and facilitate enhancements. This model evaluates the maturity of processes within the organisation and delineates steps necessary for their advancement. Typically, the CMM comprises five stages, each representing varying maturity levels, as depicted in Table 2.3 by Acohido (2015).

Table 2-3: Description of CMM stages (Acohido, 2015)

Stage	**Description**
Level 1: Initial or basic	Information security efforts are often sporadic, with a lack of formalised information security programs in most cases. A very minimal or basic level of information security controls are in place.
Level 2: Developing or evolving	Informal responsibilities are assigned to an individual who is developing an information security program, policies, and procedures. Informal communication around information security issues is taking place. Information Security Controls are inconsistently applied.
Level 3: Defined or established	Policies and procedures are defined, and roles and responsibilities are defined, but with minimum accountability or enforcement
Level 4: Managed or advanced	Clearly defined Information security roles and responsibilities with a formal information security committee consisting of business and operations managers. Information Security Controls are consistently applied
Level 5: Optimising or leading	Business have accepted the residual risk linked to their utilisation of information and technology. Full accountability from business for information security failures or policy and procedure violations. Ongoing self-improvement processes are in place and subject to regular review and updates. The company has an information security-aware culture.

As elucidated by Acohido (2015), the Capability Maturity Model (CMM) enhances the efficiency and efficacy of information security programs. It achieves this by prioritising the development of comprehensive processes that can evolve to become more automated and seamlessly integrated into

the organisation's overall operational infrastructure. Figure 2.2 provides an illustrative example of a CMM in action, showcasing how it delineates the stages of maturity and the corresponding progression towards optimised security practices.

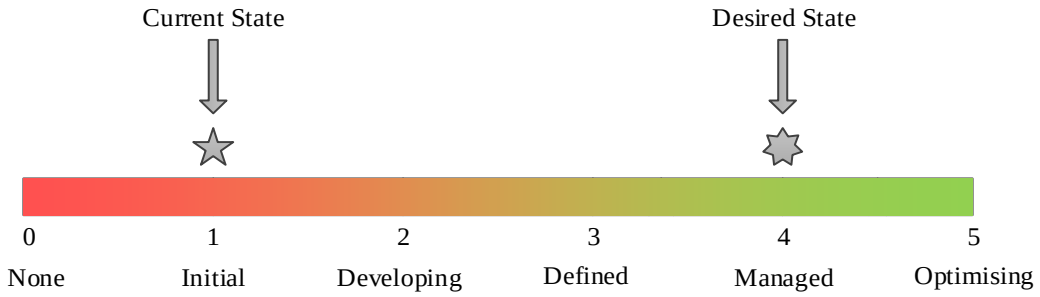


Figure 2-2: CMM example

Adapted from: Acohido (2015)

For an organisation to be considered mature, it must achieve a rating of level 5 on the CMM scale. However, according to Acohido (2015), this is for a world-class organisation that sets the benchmark for similar businesses. The maturity model is crucial in helping organisations understand their risk profile. By evaluating the potential impact of specific events on the organisation and considering their impact on its mission, asset protection, legal obligations, operational continuity, individual safety, and risk tolerance, organisations can adjust their maturity levels to accurately reflect their risk profile (U.S. Department of Homeland Security, 2015). The U.S. Department of Homeland Security (2015) outline three levels of potential impact within the maturity model for organisations:

- **LOW**: Based on the available threat intelligence, the organisation or domain area would experience minimal adverse effects.
- **MODERATE**: The threat intelligence indicates that the organisation or domain area would experience significant adverse effects.
- **HIGH**: The organisation or domain area would face severe or catastrophic adverse effects, as highlighted by the threat intelligence provided.

They also rank cybersecurity as high. This indicates that a maturity model between levels 4 and 5 needs to be implemented. Bandara, Vidanagamachchi, and Wickramarachchi (2019) indicated a desired maturity level of 4 for IIoT used in the banking industry for technology and resources, strategy and organisation, operations, employees, and governance. Kour, Karim, and Thaduri (2020) found in their assessment of the cybersecurity capabilities of railway organisations that two of the three had their cybersecurity management and identity and access management at a maturity level 4. Considering the above, the desired state for an organisation in South Africa's transport sector should be at level 4. Organisations can adjust the level based on their risk profile.

2.2.4 Information Security Frameworks and Standards

Internationally there are more than a couple of control frameworks to govern and secure IT in an organisation. The most common ones are listed in Table 2.4. Although these frameworks are generic and can be applied across different sectors, it might not specifically address IIoT risks, threats, and vulnerabilities. There are frameworks that are more suited for IIoT as listed in Section 2.4.7.

Table 2-4: Information Security Frameworks

Control framework	Brief description	Reference
COBIT (COBIT 2019)	Control Objectives for Information and Related Technology (COBIT)	ISACA (2018)
ISO/IEC 27002:2022	International Organization for Standardization/International Electrotechnical Commission	(ISO/IEC, 2022)
ITIL version 4	Information Technology Infrastructure Library (ITIL)	(ITIL, 2022)
SANS 20 critical controls	SANS Institute developed the Center for Internet Security (CIS) Critical Security Controls	(SANS Institute, 2016)
NIST	National Institute of Standards and Technology	(NIST, 2019)

2.2.5 South African Information and Cybersecurity

SA ranks as the most targeted country for ransomware and email attacks in Africa (Seacom, 2023). The Federal Bureau of Investigation (FBI) ranked SA 11th out of 50 countries in 2014 that reported Internet-based complaints (Federal Bureau of Investigation 2014); however, in 2023, cybersecurity company and VPN provider Surfshark placed SA 5th globally according to cybercrime density, the proportion of cybercrime victims within a defined population of internet users (ITWeb, 2023).

According to the global Allianz report (Allianz Global Corporate & Specialty, 2023), cybersecurity risk ranks second most significant business risk in SA for 2023, with loadshedding blackout topping the list at number one. According to IOL News, 75% of South African businesses received more email-based attacks. Furthermore, SA experiences the highest incidence of targeted ransomware and business email cyberattacks across Africa, which cost SA economy around R2.2 billion a year (Matlhabe, 2022). Alfreds (2016) indicated that South African organisations are unprepared and ill-equipped to handle emerging cyber threats as they rely on outdated protection.

According to Hubeschle (2011), cybercrime was classified as a priority crime in SA by the Hawks, which is the Directorate of Priority Crime. It is still considered a Priority Crime Specialised Investigation as part of its vision, mission, and mandate (Directorate for Priority Crime Investigations, 2024). IOL News reported that SA businesses must prioritise cyber defence (Bolzonello, 2023).

IT News Africa (2018) highlighted security as a top trend and emphasises the need for robust security measures in IIoT deployments. As IIoT devices and networks become more interconnected and integrated into critical infrastructure, they become potential cyberattack targets. It emphasises the

significance of protecting IIoT systems from threats like unauthorised access, data breaches, and disruption of operations. Security should be considered upfront during design of IIoT systems (IT News Africa, 2018).

2.2.6 South African Incidents

There have been numerous cyberattacks or incidents in SA in recent years. Below are some of the more significant attacks listed in Table 2.5. These incidents highlight the importance of cybersecurity and its impact on South Africa. Increased attacks might also increase the likelihood of IIoT being impacted overall. In Sections 2.3.6 and 2.3.7, more relevant incidents to IIoT and the transport sector are discussed, along with their impact.

Table 2-5: List of South African Incidents

Attack	Description
Ransomware	According to Seacom (Seacom, 2022), eighty percent of organisations in SA have documented ransomware incidents within the past two years. SA ranks as the most targeted country for ransomware and email attacks in Africa, making it one of the top five cyber threats in the region (Seacom, 2023).
Development Bank of SA	The Development Bank of Southern Africa (DBSA) fell victim to a ransomware attack in June 2023, which significantly disrupted its operations. The attack targeted the DBSA's systems, encrypting data and demanding a ransom for its release. The bank took immediate action to isolate the affected systems and launched an investigation to assess the extent of the breach (Greig, 2023).
City Power	In 2019, Johannesburg's electricity provider, City Power, was victim to a ransomware attack, which affected a quarter of a million residents who were unable to purchase prepaid electricity (BBC News, 2019).
Transnet	In 2021, Transnet was debilitated by malware. This is further discussed in Section 2.3.7.2.
TransUnion	In March 2022, TransUnion SA was targeted by the hacker group N4aughtysecTU. After successfully breaching four terabytes of data, the group demanded a ransom of R225 million. This cyberattack compromised 54 million personal data records, as reported by BusinessTech (2022).
Shoprite	In June 2022, Shoprite, a prominent Southern African supermarket chain, was the victim of a ransomware attack. The perpetrators, RansomHouse, reportedly obtained 600 gigabytes of data, including sensitive information such as names and ID numbers. The group then demanded that the supermarket chain negotiate for a ransom payment (Moyo, 2022).
Spyware Attacks	According to cybersecurity company Kaspersky, between the final quarter of 2022 and the initial quarter of 2023, SA experienced an 18.8% surge in spyware attacks. Users across various organisations in SA remain susceptible to spyware threats on different types of devices (Ndlovu, 2023).
The National Department of Water Affairs	In June 2011, the National Department of Water Affairs systems got hacked via password fraud, causing the Department to lose R2.84 million (Patrick, 2016).
South African Postbank	• The SA Postbank's financial systems were compromised in 2021, and R42 million was stolen via mule accounts (Rasool, 2012). • Postbank experienced another malicious cyberattack in 2022, resulting in a loss of R77 million. The breach is believed to have been carried out by one of its contractors. (Maliti, 2023).
Gautrain Management Agency	In November 2014, the bank account of the Gautrain Management Agency fell victim to hacking, nearly resulting in the theft of R800 million (Patrick, 2016).
Eskom	Eskom's payroll system was almost hacked in November 2014 by two of its employees but was foiled by the Hawks. (Patrick 2016).

Attack	Description
Road Traffic Management Corporation (RTMC)	In October 2015, the RTMC bank account was hacked, and R8.5 million (Mkhwanazi, 2015) were stolen. Five people believed to be part of a syndicate were arrested for fraud and corruption.
Anonymous Africa DDoS	A hacker called Anonymous Africa performed a distributed denial of service DDoS attack on the African National Congress (ANC) and Independent Online (IOL) websites in June 2013 and the South African Broadcasting Corporation (SABC) website in June 2016 by taking them offline (Vermeulen, 2016b). Also, in June 2016, Anonymous performed a DDoS attack on Gupta-owned websites, including The New Age (newspaper), ANN7 (news channel), and Sahara and Oakbay Investments (Solomon, 2016). This was a statement by the hacktivist group against corrupt parties and corporations.
Anonymous Operation Africa (#OpAfrica)	Anonymous hacked the Government Communications and Information Services (GCIS) database in early 2016. The hacker group released the personal details of 1500 employees, including their names, email addresses, phone numbers and password hashes as part of "Operation Africa" or #OpAfrica. Operation Africa is said to focus on internet censorship and child labour (Vermeulen, 2016a). In July 2016, Armscor, the acquisition organisation for the South African Department of Defence, was hacked. Anonymous hacked its website to breach the settlement and invoicing system. Details of access to 19 938 supplier IDs, names and passwords have been leaked (Fripp, 2016; Van Zyl, 2016). The hacktivists used a simple SQL injection to hack and breach the data. This was part of the hacktivists' plan to target corrupt African governments, as Armscor was in the news about a contentious tender for a VIP Aircraft for the South African government.

2.3 Internet of Things (IoT) and Industrial Internet of Things (IIoT)

This section offers an outline of ICS/SCADA, IoT, and IIoT systems, highlighting the distinctions between IoT and IIoT and the variances between ICS/SCADA environments and IoT and IIoT. Previous versions of this section were published as an academic journal in the *Journal of Information Warfare* in July 2020 (Pretorius & Van Niekerk, 2020) and the *14th International Conference on Cyber Warfare and Security* (ICCWS) in March 2019 (Pretorius & Van Niekerk, 2019). In addition, aspects of this literature were also presented at the South African Institute of Electrical Engineers (SAIEE) in March 2019, CISO Alliance Durban Chapter in July 2019 and ITWeb Security Summit in 2020.

2.3.1 Overview of ICS/SCADA

As outlined by Stouffer, Falco, and Kent (2006), Industrial Control Systems (ICS) represent a diverse array of systems encompassing Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), including ancillary components like Programmable Logic Controllers (PLC). They are predominantly deployed within critical infrastructure and industrial domains, serving as the backbone of operations across sectors, including oil and gas, automotive, chemical, food, transportation, water, electrical, pharmaceutical, paper, and manufacturing.

ICS and SCADA systems are pivotal in operations and industries, enabling control, monitoring, and automation. SCADA caters explicitly to operational systems dispersed over vast geographical areas, exemplified by systems managing conveyor belts and similar infrastructure (Byres, 2012). They are

also pivotal in critical national infrastructure, including managing electricity grids, pipelines, and power generation facilities (Miller & Rowe, 2012; Chileshe & van Heerden, 2012).

2.3.2 Overview of IoT and IIoT

2.3.2.1 IoT

As the 4th industrial revolution unfolds, IoT is experiencing an unprecedented surge, with a continuous proliferation of internet-connected devices, gadgets, and objects. Initially, projections by Gartner (2017) anticipated a staggering 20 billion things added to the internet by 2020. However, the growth trajectory was impacted by the COVID-19 pandemic, leading to a slightly lower count, with statistics from 2022 indicating 16.4 billion IoT devices. Nonetheless, a new forecast by Weston (2023) suggests that IoT-connected devices are poised to surpass 30 billion by 2025.

While a significant portion of these devices caters to consumer needs, businesses and industries are increasingly delving into the potential of IoT devices within their respective sectors to gain a competitive advantage. Consumer-oriented IoT devices span wearables, smart homes, appliances, and vehicles, reflecting the widespread integration of IoT technologies into daily life.

2.3.2.2 IIoT

The Industrial Internet of Things (IIoT) encompasses many IoT devices that monitor and control industrial processes across diverse sectors, including transportation, manufacturing, retail, energy, operations, and healthcare. When IIoT becomes increasingly integrated with business operations, it intersects with other cutting-edge technologies, such as cloud computing and mobile platforms, augmenting design complexity and inherent risks.

The onset of the COVID-19 pandemic catalysed governments and businesses worldwide to reevaluate their objectives and operational methodologies, sparking a surge in technological innovation (Fortune Business Insights, 2023). One notable trend is the fusion of IoT with blockchain technology, leveraging the capabilities of IoT devices to gather extensive data for processing, while blockchain ensures the secure management of this data. For businesses, the primary aim of IoT deployment is to furnish executives with valuable insights derived from data analysis, aiding in informed decision-making. Additionally, IoT provides intuitive dashboards and visualisations to monitor Key Performance Indicators (KPIs) (Hitachi, 2017).

However, amidst the proliferation of IoT and IIoT, it is crucial to underscore the critical importance of information and cybersecurity. As articulated by IT News Africa (2018), security emerges as a top priority in the future trajectory of IIoT. With IIoT devices and networks becoming increasingly interconnected and integrated into critical infrastructure, they become prime targets for cyberattacks. It underscores the urgent necessity of fortifying IIoT systems against potential threats, including

unauthorised access, data breaches, and disruptions to operations. Consequently, security measures must be ingrained into the design and implementation of IIoT systems right from their inception (IT News Africa, 2018).

2.3.2.3 IIoT Components

An IIoT system typically comprises three levels: devices/sensors, gateways, and data systems (Sakovich, 2023).

Devices contain smart sensors for data collection, including temperature, pressure, humidity, light intensity, moisture levels, proximity, and RFID tags (Rajiv, 2022).

Gateways manage data flow between networks and protocols, ensuring seamless communication among devices and sensors. They can preprocess data locally to address compatibility issues before transmission (Rajiv, 2022).

Data systems, such as data centres or the cloud, handle the vast data generated by IIoT devices. They enable efficient collection, processing, management, storage, and real-time access to data. Predictive analytics capabilities empower companies to enhance products and services, implement preventive measures, and develop new business models (Rajiv, 2022).

Data transmission within an IIoT system occurs through various channels, as outlined by Sakovich (2023).

Firstly, device-to-device (D2D) communication enables direct interaction between intelligent objects, facilitating instantaneous information sharing without intermediaries. For instance, industrial robots and sensors establish direct connections to coordinate actions and enhance component assembly efficiency. While yet to be widespread, this type of connection is hindered by the limited capability of most devices to handle complex processes.

Secondly, device-to-gateway communication involves data transmission between gateway nodes and sensors. Gateway nodes, more influential computing devices than sensors, serve two essential purposes: consolidating sensor data for routing to the relevant data system, analysing data to detect issues, and sending feedback to the originating device. The choice of IIoT gateway protocols hinges on gateway computing capabilities, network capacity, data generation frequency, and data quality, ensuring optimal solutions for specific scenarios (Sakovich, 2023).

Next, gateway-to-data systems communication entails data transmission from gateways to the appropriate data system. Protocol selection for this communication type depends on connectivity frequency, congestion, security requirements, and the number of parallel connections needed.

Lastly, data systems communicate with each other within data centres or cloud environments. The protocols used for this connection should be easy to deploy, integrate seamlessly with existing applications, and ensure high availability, capacity, and robust disaster recovery capabilities to guarantee efficient and reliable data transmission (Sakovich, 2023).

2.3.2.4 IIoT Networks

IIoT networks are classified based on the distance range they cover, as indicated by Sakovich (2023). These categories, defined in Table 2.6 and depicted in Figure 2.3, encompass various types of networks.

Table 2-6: Type IIoT Networks

Network	**Definition**
Nano network	Collection of small devices, typically measuring only a few micrometres, capable of performing basic tasks such as sensing, computing, storing, and actuation. These systems find applications in various fields, including biometrics, military technology, and other nanotechnologies.
BAN (Body Area Network)	Designed to connect wearable computing devices. These devices can be worn on the body, placed in various positions nearby, or even implanted inside the body.
PAN (Personal Area Network)	Links devices within a radius of approximately one or a few rooms
LAN (Local Area Network	Covers the network area within a single building
CAN (Campus/Corporate Area Network)	A network that connects smaller local area networks within a defined geographical area such as an enterprise or a university campus.
MAN (Metropolitan Area Network)	A large-scale network that spans a specific metropolitan area and uses microwave transmission technology.
WAN (Wide Area Network)	Relates to a network encompassing a vast geographical area and connecting smaller networks, including LANs and MANs (Sakovich, 2023).

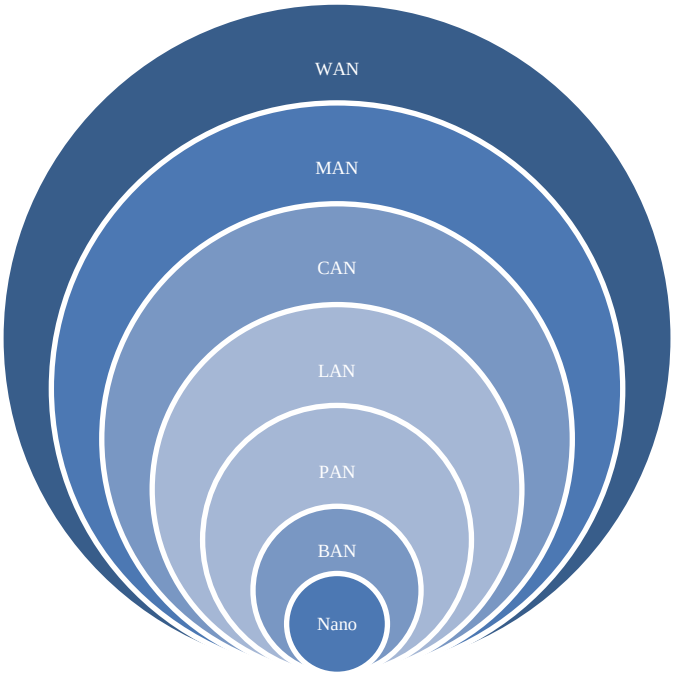


Figure 2-3: IoT Networks

Adopted from: (Sakovich, 2023)

2.3.2.5 IIoT Communication

There are various IIoT communication protocols. Below are the most common ones:

- **Wired** - Ethernet is commonly used for LANs, with different standards offering high-speed data transmission (C&T RF Antennas Inc, 2021).
- **Wi-Fi** - When it comes to integrating IIoT devices, Wi-Fi is often considered the top choice given its robust infrastructure. With rapid data transfer speeds and the capability to manage substantial data volumes, the widely adopted Wi-Fi standard 802.11 allows for the transmission of hundreds of megabits of data per second. Wi-Fi typically operates within a range of about 50 meters and supports internet protocol standards, which enables access to IoT Cloud infrastructure. It uses the 2.4GHz and 5GHz frequency bands, making it a popular choice for many IoT applications. (Hasan, 2023).
- **Bluetooth and Bluetooth Low-Energy (BLE)** – BLE is a wireless protocol frequently used in IoT devices. It offers the same range as traditional Bluetooth but consumes less power, making it an efficient and reliable way for devices to communicate with each other (Hasan, 2023).
- **Message Queue Telemetry Transport (MQTT)** - is a messaging protocol for IIoT devices for remote monitoring and data collection. It operates on a hub-and-spoke architecture and relies on TCP for reliable communication. The three key components are Publisher, Subscriber, and Broker. The Publisher generates data, the Broker facilitates communication,

and the Subscriber receives data. MQTT ensures data security by verifying authorisation. It is a reliable and scalable protocol for IIoT applications (Hasan, 2023).

- **Constrained Application Protocol (CoAP)** - For resource-constrained smart devices, Constrained Application Protocol (CoAP) emerges as a tailored solution for networks comprising similar constrained devices, including those within restricted networks. Leveraging the lightweight UDP protocol, CoAP ensures efficient data transmission, which is particularly suitable for IIoT systems reliant on HTTP protocols. Its adoption of a RESTful architecture enhances ease of use and compatibility (Hasan, 2023).
- **Advanced Message Queuing Protocol (AMQP)** - an open standard which facilitates exchange of business messages between applications or organisations. By establishing connections and delivering essential information, AMQP supports business processes and ensures reliable transmission of instructions to achieve objectives (Tezer, 2013).
- **ZigBee** - predominantly utilised in industrial settings, operates at 2.4GHz frequency, which is ideal for transmitting data between homes or buildings at low rates. Renowned for its security features, ZigBee offers scalable solutions with low power consumption, making it a preferred IIoT security protocol (Hasan, 2023).
- **Near-Field Communication (NFC)** - facilitates low-speed network connections among electric devices within close proximity. It is commonly employed in key access, contactless payments, and ID documents (Sakovich, 2023).
- **Data Distribution Service (DDS)** - enables high-performance, scalable, real-time communication between machines. Comprising Data-Centric Publish-Subscribe (DCPS) and Data-Local Reconstruction Layer (DLRL), DDS facilitates information delivery to subscribers and provides access to the mechanism's functionalities (Hasan, 2023).
- **Z-Wave** - geared towards home automation, utilises low-power RF communications, offering features that safeguard against interference from wireless technologies. In the sub-1GHz frequency band, Z-Wave prioritises straightforward development processes for IoT protocols (Hasan, 2023).
- **6LowPan** - short for IPv6 over Low-power Wireless Personal Area Networks, is an adaptation layer enabling IPv6 communication over IEEE802.15.4 links. Operating within the 2.4 GHz frequency range, 6LowPan offers a transfer rate of 250 kbps (Postscapes, 2020).
- **Cellular** – encompasses GSM/3G/4G/5G/LTE technologies, suitable for IoT applications requiring long-distance operation and transmission of large data volumes (Hasan, 2023).

Table 2.7 lists the advantages vs disadvantages of each IIoT communication protocol.

Table 2-7: IIoT Communication Advantages vs Disadvantages

Protocol	Advantages	Disadvantages
Wired	• High-speed and reliable communication • Enhanced security as the communication is not easily intercepted	• Limited mobility due to physical connections • Requires physical infrastructure and installation
Wi-Fi	• Wide availability and compatibility with existing networks • Higher data transfer rates	• Higher power consumption compared to other protocols. • Limited range and signal strength
BLE	• Low power consumption, suitable for battery-operated devices • Easy and quick device pairing	• Shorter range compared to other protocols. • Limited data transfer rates
MQTT	• Lightweight and efficient, ideal for constrained devices and low-bandwidth networks • Publish-subscribe model allows for flexible and scalable communication	• Requires a message broker for communication. • Lack of built-in security mechanisms
CoAP	• Explicitly designed for resource-constrained devices and low-power networks • Efficient use of network resources	• Limited adoption and compatibility compared to other protocols. • Lack of built-in security features
AMQP	• AMPQ is efficient, portable, multichannel, and secure. • AMPQ is highly effective in multi-client environments as it offers a way to assign tasks and enables servers to respond quickly to urgent requests.	• Older versions are not compatible with it. • It is more complex than HTTP 1.0, HTTP 1.1, or any other protocols. • Unlike MQTT/CoAP/XMPP, higher bandwidth is needed for this. • CoAP/HTTP/XMPP support resource discovery, while it is not supported with AMQP.
ZigBee	• Low power consumption, suitable for battery-operated devices • Mesh networking enables scalability and extended coverage	• Limited range and signal strength • Interoperability challenges between different ZigBee devices
NFC	• Quick and easy device pairing through proximity. • Secure communication due to short-range proximity	• Limited range, typically less than 10 cm • Slower data transfer rates compared to other protocols
DDS	• Real-time and reliable communication for time-sensitive applications • Scalability and support for large-scale systems	• Higher complexity and overhead compared to other protocols. • Requires additional development effort for implementation
Z-Wave	• Low power consumption and extended battery life • Mesh networking enables scalability and wider coverage	• Limited range, suitable for smaller areas • Proprietary technology, limited device compatibility
6LowPan	• Optimised for low-power devices and low-bandwidth networks. • Efficient IPv6 integration for seamless internet connectivity	• Limited adoption and compatibility • Lack of built-in security mechanisms
Cellular	• Wide coverage and mobility, suitable for remote and mobile applications • High data transfer rates	• Higher power consumption and cost compared to other protocols. • Limited availability and coverage in certain areas

2.3.3 IoT vs IIoT

Technological advancements on the Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices have revolutionised how humans interact with technology. However, the distinctions between IoT and IIoT devices extend beyond mere terminology or semantic differences. While a person's smartwatch failure may inconvenience the consumer, a train's braking system failure could have life-threatening consequences (Nagaraj, 2014). This highlights the criticality of the complexity of the relationship between the two domains.

There are varying perspectives on the intricate relationship between IoT and IIoT. According to Bowne (2015), delineating the similarities and differences between IoT and IIoT is not a simple task. He suggests that IoT represents a revolutionary shift, characterised by new features such as remote access, cloud computing, and machine-to-machine communication. In contrast, IIoT, existing for some time, has evolved from these innovations (Bowne, 2015). IoT primarily serves consumers, whereas IIoT is tailored for industrial applications by engineers. Initially, Carl Henning viewed IIoT as distinct from IoT (Henning, 2015a), as illustrated in Figure 2.4. However, he later revised his stance, concluding that IIoT is a subset of the IoT umbrella (Henning, 2015b).

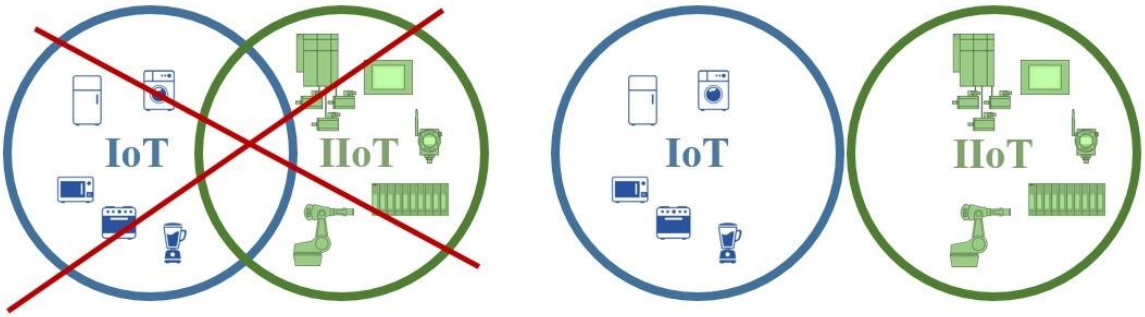


Figure 2-4: Initial view by Carl Henning

Adopted from: (Henning, 2015a)

Bowne (2015) lists the following characteristics of IoT and IIoT in Table 2.8.

Table 2-8: IoT vs IIoT

Source: Bowne (2015); Digital Directions Team (2023)

IoT	IIoT
Revolution	Evolution
Things	Data
Consumer market	Industries, e.g. manufacturing, transportation, and energy

IoT	IIoT
Ad hoc connectivity	Structured connectivity
Important –but not critical	Mission critical: • Analytics • Security (protocols, updates) • Data integrity & Encryption • Response times • Withstand environment • Access control
User serviced	User + OEM + Vendor serviced
New • Devices • Standards	Existing • Devices • Standards
Proprietary Solutions	Defined Standards

2.3.4 IoT vs IIoT vs ICS/SCADA

IIoT devices have evolved from industrial systems such as ICS and SCADA, discussed in Section 2.3.1, and were deployed in isolated networks using unique communication to standard ICT protocols connected to ICT networks. This change was driven by the need for companies to understand better their operations (Miller & Rowe, 2012). IIoT was born and evolved from traditional ICS or SCADA systems. IIoT is an excellent way for organisations to monitor their industrial and operational; these include Key Performance Indicators (KPIs) or performance analysis and predictive maintenance. Data retrieved from industrial processes have provided invaluable insights that were previously impossible to obtain. IIoT is a technology which enhances ICS or SCADA systems by building on top of it as explained by Manditereza (2017). He lists four key differences: scalability, interoperability, standardisation, and data analytics. Henning (2017) indicated that IIoT is part of IoT and Industrie 4.0, as depicted in Figure 2.5.

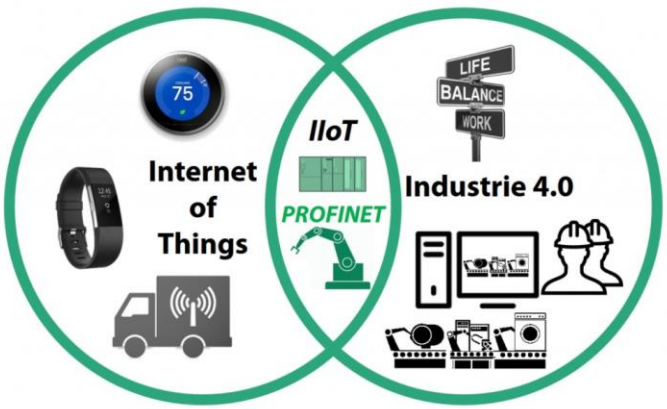


Figure 2-5:IoT vs IIoT vs Industrie 4.0

Adopted from: Henning (2017)

Considering that IIoT is an extension of ICS or SCADA systems and is also a part of IoT and Industrie 4.0, we can classify ICS or SCADA and Industrie 4.0 as operational technology. This means that IIoT is where IoT and operational technology overlap, as illustrated in Figure 2.6.

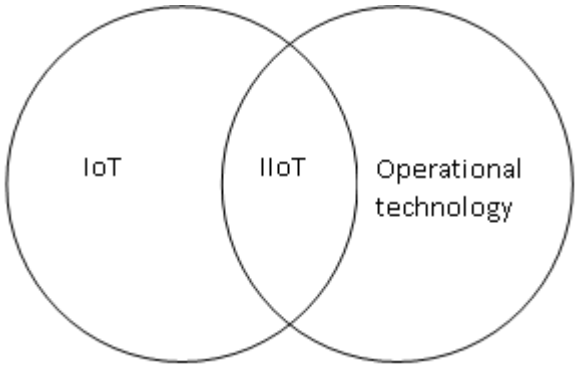


Figure 2-6: IoT vs IIoT vs Operational technology

Source: Author compiled, Adapted from: (Henning, 2017)

To understand how we can protect IIoT and IoT devices, we need to understand what incidents occurred and the associated risks, vulnerabilities, and threats. The most significant cyberattack to date, which took down over half of America's Internet, was in October 2016, caused by IoT devices infected with malware. These IoT devices were infected with malware known as Mirai botnet which took most internet websites offline (Woolf, 2016). There have been many incidents involving IoT devices, this is discussed in Section 2.4.5. These vulnerabilities, threats and risks influence the technological, organisational, and environmental factors influencing the security and governance of IIoT and IoT in South Africa.

2.3.5 Threats, Vulnerabilities and Risks

2.3.5.1 Threats

Previous studies focussed on ICS/SCADA (Pretorius, 2016) showed that the top threats were malware, staff undertaking unintentional unauthorised actions and disgruntled staff, which influenced ICS/SCADA in South Africa. These threats could cause distribution to business processes and operations and impact financial loss or probably human life. It was also found that ICS/SCADA systems are not governed and not secured in South Africa. If IIoT is an extension of ICS or SCADA systems (Manditereza, 2017), these threats and risks might be inherited by IIoT devices. There are also new threats being introduced by IIoT.

Thoroughly assessing all system components, including sensors, gateway devices, and network infrastructure, is necessary to fully understand vulnerabilities. This will help determine if any vulnerabilities exist, as CPNI (2008) advises. Based on the "Internet Security Threat Report" by Symantec in 2018, there was an alarming 600% surge in the number of attacks on IoT, from 6,000 in

2016 to a staggering 50,000 in 2017. This increase could be due to the amount of IoT and IIoT deployments. Analysing the report from Symantec (2018), the top threats witnessed by IoT honeypots in 2017 are displayed in Table 2.9 and Figure 2.7, demonstrating more than 60% of threats linked to DDoS and malware, with 26%.

Table 2-9: Top threats in IoT and IIoT deployments

Rank Threat Name	Threat type	Percent
Linux.Lightaidra	DDoS	57.5
Trojan.Gen.NPE	Malware	10.2
Linux.Mirai	Botnet	8.7
Trojan.Gen.NPE.2	Malware	4
Linux.Kaiten	DDoS	3.6
Downloader.Trojan	Malware	3
Linux.Gafgyt	Malware	2.7
Trojan.Gen.8!cloud	Malware	2.2
SecurityRisk.gen1	Malware	1.9
Trojan.Gen.6	Malware	1.7
Unknown	Unknown	4.5

Source: Symantec (2018)

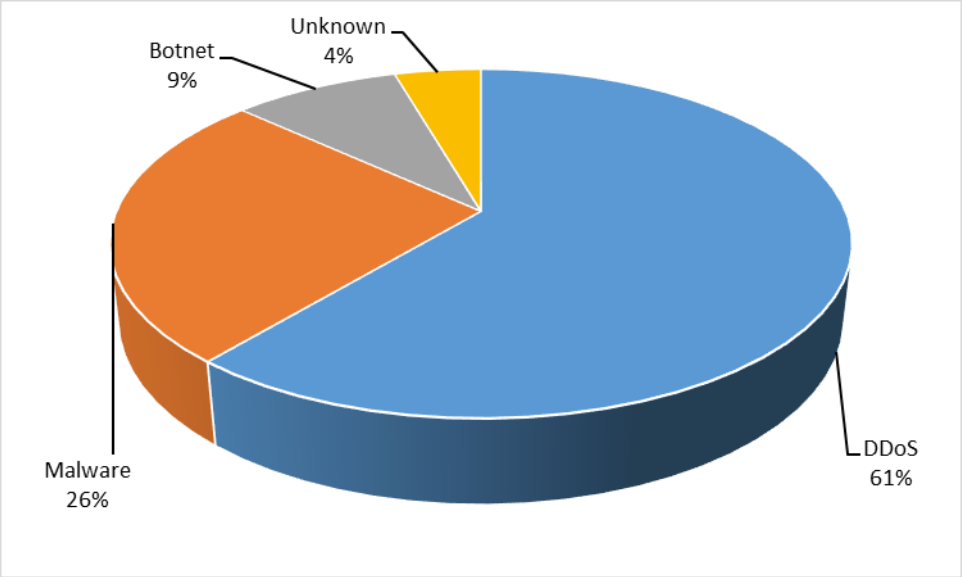


Figure 2-7: IoT and IIoT threats and attacks

Adapted from Symantec (2018)

Kaspersky's ICS CERT predicted an increased attack surface due to digitisation, ransomware attacks on critical infrastructure, and activities of cybercriminals. The expansion of digitisation in the race for advancements in IIoT and intelligence, such as predictive maintenance systems and digital twins, will increase the attack surface (CIO Southeast Asia, 2022).

According to the latest IoT Security Landscape report from Bitdefender (Bitdefender, 2023), the number one attack type was Denial of Service, which accounted for 84% of the incidents in 2022.

In the data breach digest report by Verizon (Verizon, 2023) displayed in Figure 2.8, most incidents, and breaches (53%) in the transportation sector were caused by malware, followed by Hacking (31%) and Social Engineering (8%). Verizon then clusters the threat types, e.g. malware could cause Denial of Service and System intrusion. The clustering for the threat types in the transportation sector is displayed in Figure 2.9, with 61% of breaches or incidents in the transportation sector caused by System Intrusion, followed by Denial of Service (19%) and Web application attacks (11%). This shows that DoS are both common IoT threats and threats in the transportation industry.

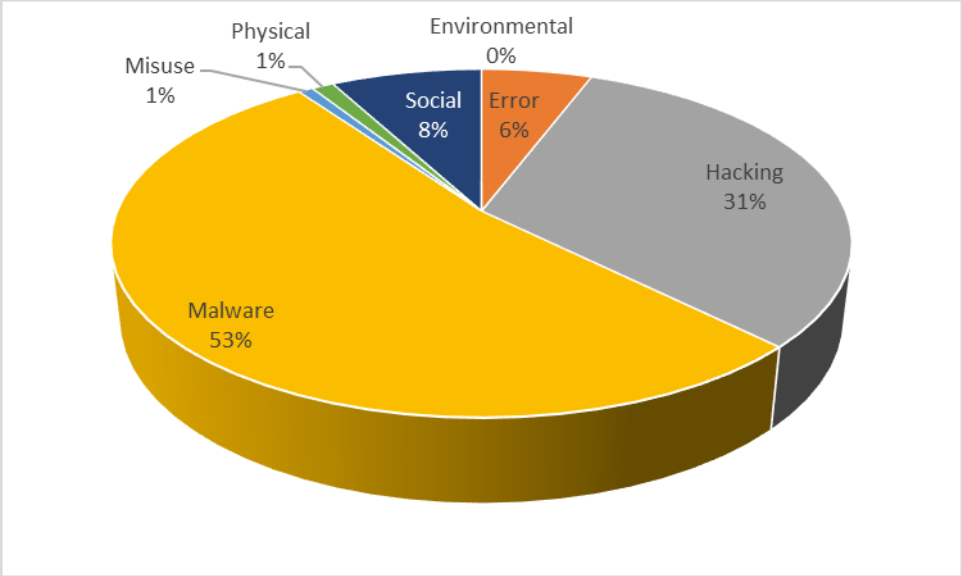


Figure 2-8: Threats in the transportation sector

Adapted from (Verizon, 2023)

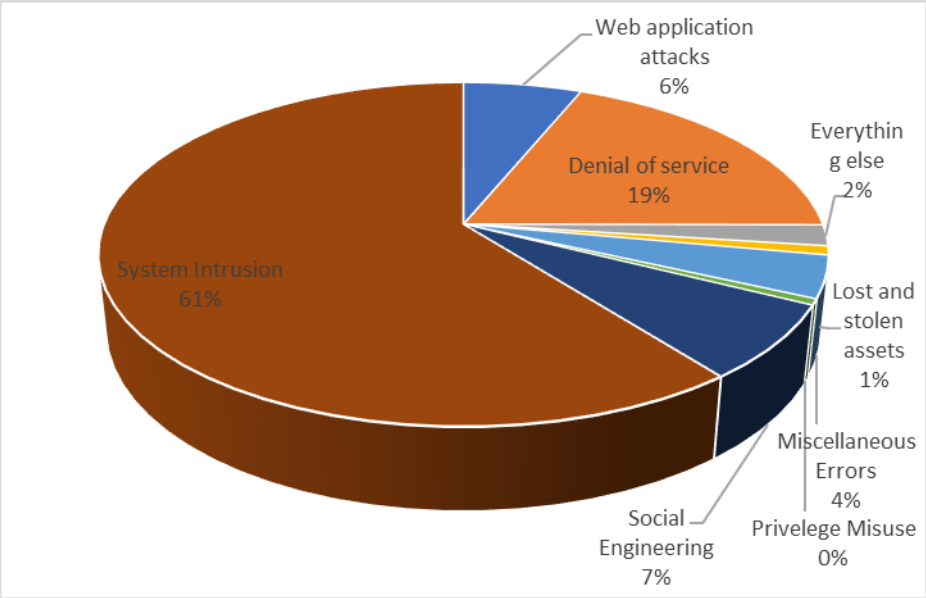


Figure 2-9: Clustering of threats in the transportation sector

Adapted from (Verizon, 2023)

The Verizon data breach digest report from 2018 grouped transportation with warehousing, and in 2019, 2020, and 2021 transportation was omitted entirely. The reports for 2022 and 2023 again contained statistics about transportation. This shows inconsistency in how incidents and breaches are reported and would make it challenging to perform trend analysis for the transportation sector.

2.3.5.2 Vulnerabilities

According to Coldewey (2019), 90% of IoT devices are manufactured without security in mind leading to vulnerabilities and potential exploitation. CPNI (2008) indicated that to fully comprehend vulnerabilities, a comprehensive assessment of all IIoT system components mentioned in Section 2.4.1.3 (devices/sensors, gateway devices, data systems) and the underlying network infrastructure must be conducted to determine whether any vulnerabilities exist.

Table 2.10 lists a summary of the common vulnerabilities listed by OWASP (n.d.), seven serious IIoT vulnerabilities listed by Franklin (2018) and the Top ten IIoT vulnerabilities by Bhattacharya (2018).

Inexpensive IIoT devices can pose significant security risks, compromising networks after being discarded. These devices, although small, function as networked computers and often lack basic security measures, exposing private information and granting unauthorised access. The lack of care in construction and code extends beyond smart bulbs to other devices, falsely claiming accreditation while neglecting safety and security (Coldewey, 2019).

Reports from Zscaler, an Internet Cybersecurity Company, reported that 91.5% of data transactions in corporate networks generated by IoT devices are unencrypted. This is a massive vulnerability as data is unprotected in transport and are susceptible to Man-in-the-middle (MitM) attacks (Constantin, 2019).

Along with the vulnerabilities mentioned earlier, Ivezic (2018) pointed out that the connection or interface between the transport engineering and passenger entertainment systems is also vulnerable. This could give hackers access to critical systems, so it is essential to isolate the two.

Chan (2017) mentioned that IIoT requires more security than commercial IoT due to the placement of IIoT in critical industrial processes; however, many connected devices may contain vulnerabilities, some of which are not disclosed by the manufacturers, in what Solomon (2022) calls “insecure-by-design”. Johnson (2017) and Ku and Weiss (2017) indicate that security IIoT is particularly challenging. Some security concerns with IIoT include authentication, insecure protocols for data transfer, insecure data storage, insecure gateways and interfaces, and supply chain risks relating to vulnerabilities in IIoT or individual components (Ku & Weiss, 2017; Sullivan, 2020).

Table 2-10: Common IIoT vulnerabilities
Adapted from OWASP (n.d.), Franklin (2018) and Bhattacharya (2018)

Category	Vulnerability
Access	Username Enumeration by interacting with the authentication mechanism.
	Unable to change default passwords.
	No Account Lockout Ability. It can allow authentication attempts after several failed login attempts.
	Improper Authentication methods or lack thereof. Lack of two-factor authentication mechanisms (e.g., security token).
	There are no password controls (password length, complexity, passwords don't expire etc.).
	Ability to obtain console access by connecting to a serial interface (e.g., USB, Ethernet port, serial port).
Patching/Firmware updates	No ability to manually force an update check for the device.
	No ability to update the device.
	Excessive access permissions allow updated files to be modified and distributed to all users.
	The current firmware version is not displayed, or the last update date is not displayed.
	Firmware contains sensitive information, such as source code, default passwords, ssh keys, and binaries of running services.
	Out-of-date versions of third-party components. E.g., Web servers, SSH or OpenSSL.
Configuration	Manipulating the code execution flow of the device. Ability to modify the execution of firmware in the device and bypass almost all software-based security controls. Side-channel attacks can also modify the execution flow or can be used to leak interesting information from the device.
Encryption	Unencrypted Network Services allow eavesdropping or tampering by attackers.
	Poorly Implemented Encryption. It is improperly configured or is not being properly updated, e.g., using SSL v2.
	Updates are transmitted over the network without using TLS or encrypting the update file itself.
Removable media	Removal of Storage Media Ability to physically remove the storage media from the device.
DDoS	IIoT can be attacked in a way that denies service to that service or the entire device via a Distributed Denial of Service (DDoS) attack.
Protocols	Certain protocols, such as MQTT, are insecure. Some vulnerabilities do not lie in the protocols themselves on the configuration and how they are implemented.
Unreliable interfaces	Flaws in the source code of the web interface cause the interface to be vulnerable to a Cyber based attack. E.g., included SQL injection, cross-site scripting, and cross-site request forgery.
	Cloud interface represents yet another potential security vulnerability.
	Unreliable mobile interface.
Privacy	Erasing personal or company data is not so easy.
	Data on the IoT device is not encrypted, which makes data vulnerable to covert hijacking and theft.

Numerous tools are available to detect vulnerable IIoT devices exposed to the Internet. Shodan is one of them. Hackers often use Shodan to search and exploit vulnerable IIoT devices. In 2019 Shodan launched a tool, Shodan Monitor, to assist companies and individuals in tracking and monitoring exposed devices on the Internet (Baran, 2019).

2.3.5.3 Risks

Bitdefender (2023) list the following three IoT risks: Cybersecurity, Privacy, and Physical safety risks. Archon (n.d.) lists risks of device hijacking, data siphoning, data breaches, Man-in-the-middle, device spoofing, and device theft. If malicious software such as ransomware or malware infects an endpoint or IIoT sensor, an unauthorised individual could gain control over the operations of the affected device. Data siphoning, like a surveillance-style attack, targets the information transmitted by an industrial IoT device instead of the end user. IIoT devices also face the possibility of a DDoS attack affecting all devices or the internal network. Data breaches for IIoT devices can also occur due to legacy or outdated systems (Okeke, 2022). Devices deployed in remote locations are especially vulnerable to physical attacks. This risk becomes more significant when endpoint devices store sensitive information that could pose a threat if it falls into unauthorised hands (Archon, n.d.).

IIoT World (IIoT World 2019) list the following ten security risks that an IIoT environment poses:

Figure 2-10: Top 10 security risks that IIoT poses

The transportation industry's adoption of IIoT and OT technologies introduces a new set of cyber risks. These technologies have a history of vulnerabilities, making the transportation industry vulnerable. Seven pressing cyber risks in the transportation industry are listed (Martin, 2022). Firstly, the reliance on third-party IIoT and OT devices without adequate security measures creates a single point of failure that cybercriminals can exploit. Additionally, the lack of visibility into the attack surface makes it challenging to secure networks and respond to attacks promptly. Insecure communications protocols used by IIoT, and OT devices allow attackers to intercept communications easily. The inadequate cybersecurity of industrial control systems makes them susceptible to attacks,

as demonstrated by incidents like the Stuxnet malware. Insufficient security controls in IIoT and OT devices make them easy targets. The lack of staff training and awareness leads to insecure usage of devices, emphasising the need for proper training programs. Finally, the absence of incident response plans can result in delays and increased damage during an attack. To mitigate these risks, transportation companies should prioritise device security, gain network visibility, use secure communication protocols, secure industrial control systems, implement robust security controls, provide staff training and awareness, and develop comprehensive incident response plans (Martin, 2022).

2.3.6 IIoT Incidents

To safeguard IIoT devices, it is essential first to understand the incidents that have taken place, as well as the risks, vulnerabilities, and threats associated with them. According to Kaspersky's ICS CERT, the rise of digitisation and the activities of cybercriminals are anticipated to result in an expanded attack surface. The push for advancements in IIoT and intelligent technologies, including predictive maintenance systems and digital twins, will contribute to this increase in vulnerabilities and incidents (CIO Southeast Asia, 2022).

Several cybersecurity incidents have occurred due to insecure IoT and IIoT devices. This section discusses key, select incidents to illustrate the range of threats and vulnerabilities relevant to IIoT devices. The most prominent cybersecurity incident was the Mirai botnet, that conducted several DDoS attacks in 2016. The infected devices that targeted service provider Dyn reportedly comprised over 100 000 devices, primarily digital video recorders, CCTV cameras, and home routers from over 160 countries. This was followed by a DDoS attack on a Liberian telecommunication provider, with traffic reaching 500GB/s. At the time, the DDoS attack was the largest recorded, and variants of the Mirai were reported to have spread to 500 000 devices that were compromised due to weak default passwords (Forrest, 2016; Kan, 2016; Woolf, 2016).

In another incident, an undisclosed university suffered a DDoS attack due to IIoT devices inside the network being compromised. The attackers gained control of the devices by using the manufacturer's default passwords, which were then changed, and brute-force attacks were conducted to compromise other devices. Approximately 5 000 devices, such as smart lightbulbs and connected vending machines, were compromised and then used to conduct a DDoS against the university's domain name server (Cimpanu, 2017). In 2017, a connected temperature sensor in a casino's fish tank was used as an entry point into the network and stole 10GB of data (Schiffer, 2017).

Standard commercial IoT devices in the household and businesses have been compromised, or concerns have been raised about their security. Digital road signage and billboards have been hacked to display messages, with warnings about weak default and hardcoded passwords that can be used to compromise such devices (Kovacs, 2014). A fridge has been seen to have sent spam emails; the FBI

released a warning about insecure baby monitors and toys as well as the risk of smart TVs or entertainment systems with a camera and microphone, which have raised privacy concerns (Lomas, 2015; Schiffer, 2017; Starr, 2014; Vaughan-Nichols, 2019). In addition, there have been reported cases where video conferencing systems have been compromised and large quantities of information stolen from organisations. This further illustrates the potential use of IIoT devices for espionage; if the audio and video could be accessed, the attackers would be able to steal sensitive corporate information (Darktrace, 2016).

A malware variant targets IoT devices and erases their firmware, reminiscent of the destructive BrickerBot malware that caused extensive damage to millions of devices in 2017 (Cimpanu, 2019). The bot is aimed explicitly at UNIX-based systems with default login credentials, leading to the infection of nearly 4000 devices and an increasing count. To restore functionality, victims must reinstall their devices' firmware, a challenging task for many device owners (Zurkus, 2019).

More concerning is that the United States Food and Drug Administration (FDA) enunciated in January 2017 that medical devices, such as pacemakers, are vulnerable (Latesthackingnews, 2017). This could cause hackers to intercept the wireless Radio Frequency signals for certain transmitters and kill patients by sending specific commands. IIoT devices have the potential not only to inflict personal damage but also have the potential to end human life.

IIoT devices themselves may not necessarily be the entry point. Vendors and third-party services may be compromised to gain access to the organisation. A significant example of this is the US market chain Target, where in 2013, cybercriminals managed to steal 40 million credit-card records after entering Target via the Heating, Ventilation and Air Conditioning (HVAC) contractor. This was one of the most significant data breaches at the time, estimated to have cost Target over 200 million USD (Zimmerman, 2017).

The above incidents illustrate several vulnerabilities, risks and threats related to IIoT. These can be seen to include DDoS attacks affecting networks, stolen data, privacy, and espionage. Vulnerabilities can include insecure protocols, and device authentication, with third parties and devices contributing to breaches.

2.3.7 IIoT in the Transport Sector

There are several benefits to IIoT in the transport sector, including automation, real-time monitoring, analytics for optimisation, improved communication, and connectivity, for example, vessels at sea, which have a potential for cost savings (Burkhalter, 2022a; Kapkaeva, Gurzhiy, Maydanova, & Levina, 2021; KVH Watch, 2021). The concept of 'smart ports' implies enhanced productivity, automation and intelligent infrastructure based on technologies such as IIoT and artificial intelligence (Min, 2022; Molavi, Lim, & Race, 2019). Molavi et al. (2019) also indicate that a measure of a 'smart

port' is an interface with intelligent railways. Ayyagari (2018) describes several benefits of IIoT in railways, like those in the maritime sector: improved monitoring translating into better safety and reliability, predictive maintenance, and analytics to aid optimisation.

Autonomous vehicles rely extensively on IIoT technologies to facilitate communication and decision-making processes (Biswas & Wang, 2023). Similarly, transport systems heavily depend on IIoT devices to enhance operational efficiency (Biswas & Wang, 2023). The physical infrastructure is critical in ensuring the reliability and safety of transportation systems (Mohebbi et al., 2020). Within the transport sector, IIoT devices are instrumental in optimising operational efficiency and responsiveness, ensuring seamless delivery of transportation services (Hindarto, 2023). Moreover, IIoT plays a pivotal role in Intelligent Transportation Systems (ITS) (Wu, Dai, Wang, Xiong, & Guo, 2022), where secure and efficient data communication among vehicles, infrastructure, and traffic management systems is imperative.

Cybersecurity for the transportation sector is essential due to its critical nature: the significance of the sector is highlighted by the US Cybersecurity and Infrastructure Security Agency (Cybersecurity and Infrastructure Security Agency, 2020), Theoharidou, Kandias, and Gritzalis (2012) and in the Australian Security of Critical Infrastructure Act (No. 29 of 2018). Akpan, Bendiab, Shiaeles, and Karamperidis (2022) raised several challenges for cybersecurity in the maritime domain, particularly surrounding automated ships: due to the number of systems for navigation, radar, communications, propulsion and the associated industrial control and IT networks, many with demonstrated vulnerabilities, makes cybersecurity of a connected vessel difficult. Similarly, automated ports could face the same challenges, as well as railways and pipelines, which often have interfaces with the maritime sector. Cybersecurity incidents demonstrating the possible attack methods and consequences are illustrated in the following section.

2.3.7.1 Cybersecurity Incidents in the Transport Sectors

The number of cybersecurity incidents affecting the transportation sector has been increasing, as indicated by van Niekerk (2017). According to IT News Africa (2022), the number of ransomware attacks in the transport and shipping industry doubled in 2022. This section discusses select incidents to illustrate the threats experienced within the sector. Numerous other security incidents have been recorded in the transportation sector (railway, maritime, air, road etc.). Although not all IIoT systems have been compromised, some have affected critical transportation infrastructure and related organisations. The most notable examples include:

2.3.7.1.1 Maritime

- Cybersecurity incidents have affected port operations, such as a DDoS attack disrupting the Port of Houston in 2001 (McCue, 2003).

- Ransomware affected port operations at Transnet in SA in 2021 (Gallagher & Burkhardt, 2021), refer to Section 2.3.7.2.
- The Not-Petya, a modified version of Petya, affected A.P. Møller-Maersk's port operations globally (Cimpanu, 2018) resulting in Maersk suffering over $300 million loss.
- A significant port terminal in Iran was disrupted by a cyberattack in 2020, attributed to a nation-state (Warrick & Nakashima, 2020).
- Ports have also been disrupted due to signal jamming of global positioning systems, such as in an undisclosed European port in 2015 and the Port of Shanghai in 2019; the latter also experienced spoofing of both global positioning system and Automatic Identification System signals (Goward, 2019; Knox, 2015).
- Criminals have used cyberattacks to track shipping containers with smuggled goods, as in the Port of Antwerp in 2013 (Dunn, 2013).
- Sea-going vessels have also been affected by cyberattacks. A series of oil rigs were affected by cybersecurity incidents, including malware disrupting the navigation systems resulting in the rig drifting off position and hackers tilting an oil rig in 2014, resulting in a disruption of operations (CyberKeel, 2014; Knox, 2015; Swanbeck, 2015; Wagstaff, 2014).
- In addition, a disgruntled insider turned off the safety systems of oil rings in 2009 (Kravets, 2009).

2.3.7.1.2 Rail

Delays in passenger rail services have been experienced due to malware (CSX Corporation in 2013), ransomware (San Francisco in 2016), DDoS (Denmark in 2018), and a network intrusion that affected the signals (United States in 2011) indicating a range of threat types can cause disruptions (Fletcher & Bye, 2022; Miller & Rowe, 2012; Ragan, 2012). Below are additional ones:

- One of the earliest attacks against a rail system occurred in Poland in 2008, when a team built a device to remotely switch the points on the tram system, resulting in a derailment (Ismail, Sitnikova, & Slay, 2015).
- In 2003, a 14-year-old boy in Lodz, Poland, caused a commotion when he used a modified TV remote to play with the tram system like it was his own train set. Unfortunately, his prank resulted in four trams derailed and 12 people getting hurt because he changed the track points. (Leyden, 2008).
- In 2003, train delays occurred due to the Sobig virus causing the shutdown of several systems within CSX Corporation. (Miller & Rowe, 2012).
- In 2017, about 450 computers belonging to German Rail (DB) were hit with the WannaCry ransomware, resulting in a demand for a $300 Bitcoin payment in exchange for access to the

affected systems. As a result of this attack, passenger information systems, ticket machines, and CCTV networks were all affected (Barrow, 2018).

2.3.7.1.3 Road

- In 2018, Bay & Bay Transportation experienced a ransomware attack that encrypted the systems responsible for managing their fleet of 300 trucks. Despite unsuccessful restoration efforts, the trucking company ultimately decided to pay a ransom amounting to five figures. Alongside the expenses incurred from recovery attempts and lost time, the incident inflicted a substantial six-figure financial impact on the business. This case starkly illustrates the exorbitant costs that trucking companies may face due to inadequate investment in cybersecurity measures (Miller A., 2021).
- In 2015, Charlie Miller and Chris Valasek, two hackers, showed how virtual carjacking can be done by taking over a Jeep Cherokee and controlling it to their liking (Greenberg, 2015). Anti-theft systems that protect against car theft can be manipulated to track, immobilise, and unlawfully acquire vehicles (Grustniy, 2019). A significant security vulnerability in GPS apps used in vehicles for tracking allowed hackers to remotely control a moving car and shut down the engine, as reported by Balaji (Balaji, 2019).
- Uber experienced a security breach in September 2022 when an attacker successfully hacked into their HackerOne account, obtained unauthorised access to a Slack account, and got complete administrative control over Uber's AWS Web Services. The initial breach was initiated through a targeted social engineering campaign aimed at Uber's employees (Georgieva, 2022).
- On September 8, 2013, a Trojan virus infected the toll plaza on Israel's Carmel Tunnels Toll Road. The virus specifically targeted the security camera system, which caused disruptions to critical operations for more than two days and resulted in financial losses. (Ashford, 2013).
- In 1992, a former Chevron employee hacked into the emergency alert network after being terminated. This resulted in the system being turned off, and unfortunately, it went unnoticed until a genuine emergency occurred, and the system did not function correctly (Miller & Rowe, 2012).
- Studies have shown that numerous vehicles are susceptible to hacking if physical access is obtained, and once compromised, certain vehicles can be remotely controlled (Higgins, 2015).

2.3.7.1.4 Pipelines

- Pipelines have also experienced disruptions from cyberattacks, most notably the ransomware infection at Colonial Pipelines in 2021, which resulted in significant social ramifications (Kerner, 2022).

- A disgruntled insider aided attackers with a backdoor, which affected flow control systems at Gazprom in 1999 (Miller & Rowe, 2012).
- Wiper malware rendered corporate computers ineffective at Saudi Aramco in 2012 but did not affect industrial systems (Bronk & Tikk-Ringas, 2013). A cyber espionage operation stole operational data from US pipeline organisations from 2011 to 2012 (Clayton, 2013).
- In 1982, there was an explosion in a trans-Siberian pipeline, reportedly caused by a logic bomb inserted into the control system, purportedly by the CIA. The explosion had a force equal to 3 kilotons of TNT (Miller & Rowe, 2012; Weiss, 2008; Andress & Winterfield, 2011).

2.3.7.1.5 Air

- The cyberattack on EasyJet is a significant reminder of cybercrime's impact on airlines. In 2020, the personal information from 9 million EasyJet customers was stolen, with credit card information compromised for 2,208 individuals. This breach, combined with challenges from the COVID-19 pandemic, resulted in a 45% decline in the airline's share value and marked its first annual loss in the 25 years since its establishment (Miller A., 2021).
- In 2018, the National Aeronautics and Space Administration (NASA) declared that their Jet Propulsion Laboratory (JPL) was breached via a Raspberry Pi, widely recognised as the next generation of IoT applications. 500MB of mission data was stolen during the ten months the hackers remained undetected (Mamiit, 2019).
- In 2009, the Conficker worm disrupted operations at a French military airfield, preventing aircraft from taking off, and affected British warships (Kirk, 2009; Willsher, 2009).
- Warsaw airport – in 2015, airplanes were unable to take off after a DDoS attack disrupted the network (Brook, 2015).
- According to reports, a researcher could hack into an aircraft's controls by exploiting its in-flight entertainment system vulnerabilities (Zetter, 2015).

The above incidents illustrate that the transportation sector has been affected by numerous threats, including DDoS, malware, ransomware, signal jamming, and other system intrusions. Threat actors include insider threats, state actors, cybercriminals, and individual perpetrators. These incidents demonstrate the reality of threats against transportation and critical systems. Such threats are not mere hype that causes unnecessary panic.

2.3.7.2 Incidents in the South African Transport Sector

In SA, we have witnessed several incidents that have influenced the physical transportation sector. Attacks on trains, burning and destroying thereof (Peterson, 2018), have increased recently. Although this is not cyber-related, criminals can use insecure IIoT devices to reveal the positions of the train and cargo. Another significant incident occurred early in 2018 when Transnet lost a container of 22

000 smartphones to criminals (Ndaliso, 2018). Although Transnet did not disclose how it occurred, criminals had to know how to bypass the Port's ICT systems and know which container contained the cargo. This could be a modus operandi like the Port of Antwerp incident (Dunn, 2013).

Tracker, a stolen vehicle recovery company, was hacked in 2020. Tracker was a target of a ransomware attack that encrypted information on their systems, disrupting over a million customers' accesses to their systems and tracking of vehicles. Tracker immediately took their systems offline when the malware was detected as a temporary precaution to stop the ransomware from spreading to other areas of its network (Moyo, 2020).

The most devastating attack on the South African transport sector was in 2021, when Transnet was incapacitated by malware speculated to be 'Death Kitty'. The logistic company overseeing South Africa's rail, port, and pipeline infrastructure faced a standstill due to a ransomware attack. Consequently, ships and trucks could not undergo processing, leading to significant disruptions in the supply chain. This incident marked the first instance of severe disruption to the integrity of South Africa's critical transport infrastructure. Employees received instructions to power down devices linked to the Transnet network amid worries about the malware spreading laterally into other vital services (Gallagher & Burkhardt, 2021).

2.3.8 IIoT Control Frameworks

Numerous IT security standards, best practices and control frameworks are provided by various organisations worldwide. These include ISACA's COBIT, SANS 20 critical controls, ISO/IEC 27002, ITIL, National Institute of Standards and Technology (NIST) SP800-82, and Centre for the Protection of National Infrastructure (CPNI) and are discussed in Section 2.2.4. Like ICS / SCADA systems, several international best practices or standards exist to govern and secure these systems (Pretorius, 2016). However, these standards do not specifically address the use of IIoT. According to Baker (2021), some IoT cybersecurity management frameworks fail to deal with cybersecurity risks effectively. Numerous standards, frameworks, and guidelines have been issued concerning IIoT standards. Each IIoT vendor typically advocates for its guidelines and standards. Consequently, various organisations, including the Online Trust Alliance, Open Connectivity Foundation, Industrial Internet Consortium (IIC), NIST, and IEEE Internet of Things, have published their frameworks and guidelines. Table 2.11 presents some of these frameworks and standards.

Table 2-11: Frameworks and standards

Source: Author compiled.

Organisation published by	Name of document	Year published
Online Trust Alliance	IoT Trust Framework	2017
Industrial Internet Consortium (IIC)	Industrial Internet of Things, Volume G4: Security Framework	2016
Open Connectivity Foundation	OCF Security FAQ and OCF 1.1.1 Security Specification	2017
National Institute of Standards and Technology (NIST)	NIST IR.8228 Consideration for Managing IoT Cybersecurity and Privacy Risks	2019
IEEE Internet of Things	P2413 - Standard for an Architectural Framework for the Internet of Things (IoT)	2015
	IEEE Standard for Health Informatics - Point-of-care medical device communication - Transport profile - Infrared	2004
Alliance for Internet of Things Innovation	AIOTI WG07 Report on Wearables	2015
	AIOTI WG09 Report on Smart Mobility	2015
International Electrotechnical Commission (IEC)	IEC/TR 62443-2-3, "Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment."	2015
Cloud Security Alliance	Security Guidance for Early Adopters of the Internet of Things (IoT)	2015
Object Management Group	DDS-Security	2016
Thread Group	Thread 1.1 Specification	2017
Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	2016
Groupe Spécial Mobile Association (GSMA)	GSMA IoT Security Guidelines	2015
US Department of Homeland Security (DHS)	Securing the Internet of Things	2016
U.S. Food and Drug Administration (FDA)	Postmarket Management of Cybersecurity in Medical Devices	2016
Microsoft	Internet of Things security best practices	Unknown

Choosing the wrong standard or no standard amidst a sea of options for standards, frameworks, and controls is risky. Any standard that fails to adequately address the risks, threats, and vulnerabilities present in the transport sector needs to be corrected. Therefore, it is of utmost importance to consider these factors when selecting a standard. The abundance of standards, frameworks, and controls available for IIoT cybersecurity can make it too easy to make the wrong choice or disregard them altogether. This demonstrates a need for a study of the risks, threats, and vulnerabilities specific to the transportation sector in SA to develop a suitable cybersecurity framework.

2.3.8.1 MITRE ATT&CK Framework

The MITRE ATT&CK ("Adversarial Tactics, Techniques, and Common Knowledge") framework is a comprehensive and globally recognised knowledge base which provides insights into the tactics, techniques, and procedures (TTPs) used by cyber adversaries during various stages of an attack (The MITRE Corporation, 2023c).

The MITRE ATT&CK framework establishes a uniform language and classification system to elucidate adversary behaviour across diverse platforms, encompassing traditional IT systems, cloud environments, mobile devices, and Industrial Control Systems (ICS). It encompasses extensive knowledge comprising documented attack patterns, tools, and methodologies utilised by malicious actors.

The MITRE ATT&CK framework is an openly accessible collection of strategies and methods used by adversaries based on real-world observations. It is a fundamental asset for crafting threat models and methodologies across a spectrum of sectors, encompassing private enterprises, government entities, and the cybersecurity realm. By creating the ATT&CK framework, MITRE aims to foster collaboration and enhance cybersecurity effectiveness, aligning with its mission of solving problems to create a safer world. The ATT&CK framework is openly accessible to anyone without any cost.

It is essential to understand the tactics and techniques used by adversaries targeting IoT devices and systems. By leveraging the MITRE ATT&CK framework for ICS, organisations can adapt and extend its principles to address the unique challenges IoT environments pose. This framework enables IoT stakeholders to enhance their security posture, detect and respond to IoT-related threats, and mitigate the risks associated with cyberattacks on IoT infrastructure (Malware News, 2020). Microsoft utilised the MITRE ATT&CK for ICS to validate their Azure Defender for IoT (Abdelaal, 2021). The ATT&CK framework for ICS was also used by the Global Cybersecurity Alliance to create an IIoT system attack tree and to understand the impact of cyber risk for IIoT (Chapman, 2022).

2.3.9 IIoT in SA

According to Engineering News (Burger, 2021), vehicle IIoT applications are gaining traction in the South African consumer market, while municipalities are adopting IIoT for intelligent transportation in the public sector. As discussed in Section 1.2, IoT deployment in SA is predicted to grow 13.5% yearly from 2024 to 2028. Despite being a rapidly expanding IIoT market in sub-Saharan Africa, SA still needs to overcome hurdles that hinder widespread adoption.

Local IoT companies in SA are expanding fast. The company IoT.nxt has raised R100 million to expand the global industry (Venktess, 2017), and SqwidNet is implementing an ultra-narrow band network, called Sigfox IoT network, to enable IoT solutions at a low cost and secure connectivity (Mybroadband, 2017). The port of Durban embraced new technology as part of the new industrial revolution to connect port assets, employees, terminal operators, and the port community and be a smart port. Drones and track and IIoT trace technology sensors have been piloted successfully at the port to track port assets such as tugs and dredgers (Mphahlele, 2016).

The physical transportation infrastructure comprises airports managed by the Airports Company of SA and various toll roads, including e-tolls. According to Krutz (2006), ports integrate SCADA and

IIoT systems into their cranes, terminal equipment, and locks. Similarly, railways have signalling, and control elements installed along the tracksides. Most of these installations underpin critical infrastructure vital to the South African economy; a significant cyberattack disrupting these industries could result in severe economic repercussions and secondary social impacts.

A study was conducted in 2021 on the use of IIoT in road freight in SA (Farquharson, Mageto, & Makan, 2021). The main effect of IIoT in road freight is increased asset visibility, but challenges remain, including high installation costs, skills gaps, and concerns about hacking and cyberattacks. Road freight managers should leverage IIoT as a strategic tool to reduce operational costs, enhance decision-making, and achieve end-to-end visibility of assets.

Discovery was honoured as the top commercial IoT solution at the MTN IoT Awards ceremony 2019 for their IIoT devices. The Discovery Vitality Drive Sensor is a telematics solution designed to gather data on drivers' behaviour for insurance and safety applications (Wright, 2020). Tracker, a stolen vehicle recovery company, also uses IIoT devices to track and recover cars. The company was hacked in 2020 (Moyo, 2020). South African National Road (SANRAL) rolled out IIoT devices in SA to help automate the toll lanes and payments of tolls via e-toll (Fourie, 2020).

MSC has implemented remote shipment tracking and container monitoring by equipping their unit with internet-connected devices. These IIoT devices gather real-time data on factors like position, temperature, and door opening to provide valuable information that empowers customers. (MSC, n.d.).

2.3.10 South African Legislation

According to Seacom (2023), SA is the most targeted country for ransomware and email attacks in Africa. Additionally, based on cybercrime density, which measures the percentage of cybercrime victims among a specific number of internet users, SA is ranked 5th globally (ITWeb, 2023). Cybersecurity risk is listed as the number two business risk in SA for 2023, according to the global Allianz report (Allianz Global Corporate & Specialty, 2023).

SA is ranked on the lower end of the maturing stage because mechanisms and groups to address cybercrime still need to be implemented. The Cybercrimes Act (Government of Republic of South Africa, 2020) and the Protection of Personal Information Act, 2002 (POPI) (Government of Republic of South Africa, 2013) have recently been finalised. The United Kingdom (UK) government has released a code of practice to help companies designing Internet of Things (IoT) devices to entrench security into the design of their devices (Government of UK, 2018). There is a need to future-proof new technologies; however, IoT security has not been included in the SA Cybercrimes and Cybersecurity Bill, although SA has been pushing ahead with the fourth industrial revolution.

Several South African legislation and frameworks relate to critical infrastructure protection in which IIoT, IoT and ICS/SCADA play a role. These include the National Key Point Act, which defines critical infrastructure and resource security. Regulations for electronic communications are provided by the Electronic Communications and Transmissions (ETC) Act (Government of Republic of South Africa, 2002a) and outlines prohibited actions and basic security. Prohibited activities encompass intentional interference with electronic communications, which extends to communications among IIoT devices, systems, and their respective components.

The Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) Act (Government of Republic of South Africa, 2002b) is also applicable to IIoT that uses cellular connectivity, as discussed in Section 2.4.1.5. These units contain subscriber identity module (SIM) cards, so they must adhere to the RICA Act.

The Protection of Personal Information (POPI) Act (Government of Republic of South Africa, 2013) requires protecting and safeguarding personal and corporate data by ensuring the safeguarding of the information. Specific IIoT systems store critical data within their databases, and vendors may possess access to this data or sensitive configuration details. If situations like these arise, it is imperative to establish measures that guarantee adherence to the law.

The National Cybersecurity Policy Framework provides resources for the national and sector response teams, the National Cybersecurity Advisory Council, and other related initiatives. Furthermore, a draft Cybercrimes and Cybersecurity Bill (Government of Republic of South Africa, 2015) has been released and potentially impacts the IIoT environments in SA if enacted. From a governance perspective, King IV (Institute of Directors in Southern Africa, 2009) assign accountability to an organisation's board members. Ensuring that IIoT systems are well-secured to meet these requirements is crucial.

When there are too many options for standards, frameworks, and controls, there is a higher chance of selecting the wrong one or none at all. Therefore, it is essential to have a methodology and guidelines for selecting and developing these for IoT and IIoT specifically tailored to an organisation's risks, threats, and vulnerabilities while considering South African legislation.

2.3.11 Challenges

The similarities and differences between IoT and IIoT still need to be fully understood. There are differing views on the relationship between IoT and IIoT. According to Bowne (2015), it needs to be clarified where the similarities and differences lie between IIoT and IoT.

Despite being a rapidly expanding IoT market in sub-Saharan Africa, SA still needs to overcome hurdles that hinder widespread adoption. The challenges include limited awareness of the business

advantages of IIoT, apprehensions regarding cybersecurity, insufficient resources and scarce skills, and difficulty demonstrating a return on investment (Burger, 2021).

The differences between IoT, IIoT and ICS/SCADA discussed in Section 2.3.4 result in several challenges that need to be considered when developing a cybersecurity framework for the transport sector in South Africa. In addition, the current cybersecurity frameworks for IIoT do not necessarily address the threats, vulnerabilities and risks in the transportation sector and the legal and regulatory requirements specific to South Africa, as discussed in Section 2.4.10.

The complexity of IIoT architecture makes it difficult to monitor and secure. Networks can range from Nano to WAN, as described in Section 2.3.2.4, and the communication protocols vastly differ from IT or ICS/SCADA. This increases the attack surface considerably.

ICS and SCADA systems are often managed by engineering teams instead of IT departments. However, IT security teams may have limited control when securing the Industrial Internet of Things (IIoT) devices within the ICS/SCADA setup. Ensuring compliance with IT policies, standards, and frameworks can be a complex task, and obtaining the support of stakeholders can be challenging. This is particularly true when considering the potential business impacts of implementing security measures.

2.4 Previous Research

Although several studies have been conducted locally and internationally on IIoT, they have yet to specifically address the cybersecurity aspects of IIoT in the transportation sector. Furthermore, there is a lack of international studies focusing on IIoT in transportation. Existing local studies primarily examine the use of IIoT in road freight without a specific emphasis on security. These studies suggest leveraging IIoT for operational cost reduction, enhanced decision-making, and asset visibility in road freight (Farquharson et al., 2021). It is essential to conduct research that focuses explicitly on addressing IIoT security concerns. Other local studies have focused on data security, privacy, and consumer IoT devices (Ngwenya & Ngoepe, 2020). Meanwhile, an industrial IoT framework developed by Jansen (Jansen & Van der Merwe, 2020) lacks substantial cybersecurity coverage.

As evident from the limited findings on Google Scholar, Web of Science, ResearchGate, JSTOR, Acedemia.edu, journals.co.za and Semantic Scholar there is a gap in research on IIoT security in the SA transportation sector. The only three studies found on IIoT cybersecurity related to the SA transportation sector are from the author. The results are summarised in Table 2.12 below.

Table 2-12: List of previous research

Title	Citation	Sector	Country	Gaps
IIoT security: Do I really need a firewall for my train	(Pretorius & Van Niekerk, 2019)	Transportation	South Africa	None – Conference paper by the author emanated from the study
Industrial Internet of Things Security for the Transportation Infrastructure	(Pretorius & Van Niekerk, 2020)	Transportation	South Africa	None – Journal by the author emanated from the study
IOT and IIOT Security for the South African Maritime and Freight Transport Sectors	(Pretorius & Van Niekerk, 2023)	Transportation	South Africa	None – Journal by the author emanated from the study
Effect of internet of things on road freight industry	(Farquharson, et al., 2021)	Road Freight	South Africa	IIoT and security is very briefly mentioned.
A Framework for Industrial Internet of Things	(Jansen & Van der Merwe, 2020)	General	South Africa	Minimal mention of cybersecurity or focus on transportation.
A framework for data security, privacy, and trust in "consumer internet of things" assemblages in South Africa	(Ngwenya & Ngoepe, 2020)	Consumer IoT	South Africa	Not focusing on IIoT nor transportation.
A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS	(Figueroa-Lorenzo, Añorga, & Arrizabalaga, 2020)	General	Spain	Not focusing on transportation or South Africa.
Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges	Gebremichael et al., 2020	General	Sweden	Not focusing on transportation or South Africa.
The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure	(Bhaiyat & Sithungu, 2022)	Critical Infrastructure	South Africa	Not focusing on transportation.
A Security Analysis Method for Industrial Internet of Things	(Mouratidis & Diamantopoulo , 2018)	General	UK	Not focusing on transportation or South Africa.
A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT	(Sengupta, Ruj, & Bit, 2020)	General	India	Not focusing on transportation or South Africa.
Towards effective security control assignment in the Industrial Internet of Things	(Hassanzadeh, Modi, & Mulchandani, 2015)	General	USA	Not focusing on transportation or South Africa.

2.5 Summary

Information Security, its vulnerabilities, threats, risks, and controls, in general, are discussed. Internationally cybercrime has increased, and in SA, millions have fallen victim to cybercrime. SA has the most ransomware attacks in Africa, which cost the SA economy around R2.2 billion a year.

The vulnerabilities and threats for to IIoT are discussed. As demonstrated by incidents discussed, the IIoT environment is vulnerable to attacks, resulting in significant disruptions.

SA has several IIoT implementations in critical infrastructure, discussed in Section 2.3.9, that are vital to the economy; it is, therefore, important that these are protected. Security in the IIoT environment faces several challenges. There exist international control frameworks; however, these do not address the South African transport sector, nor are they aligned with South African legislation. The next chapter discusses the research methodology.

Chapter 3 Methodology

3.1 Introduction

This chapter highlights the research problem, research design in the research onion, conceptual framework, framework development methodology and questionnaire design. The Business Model for Information Security (BMIS) conceptual framework will guide the study. BMIS serves as a framework for addressing various dimensions of information security within organisations, which includes the technological, organisational, procedural and people aspects. The sampling strategies are explored, such as the population, size, and data collection methods. Data analysis, conceptual framework, and questionnaire design are mentioned. Figure 3.1 is a graphical representation of the outline of this chapter and its overall structure.

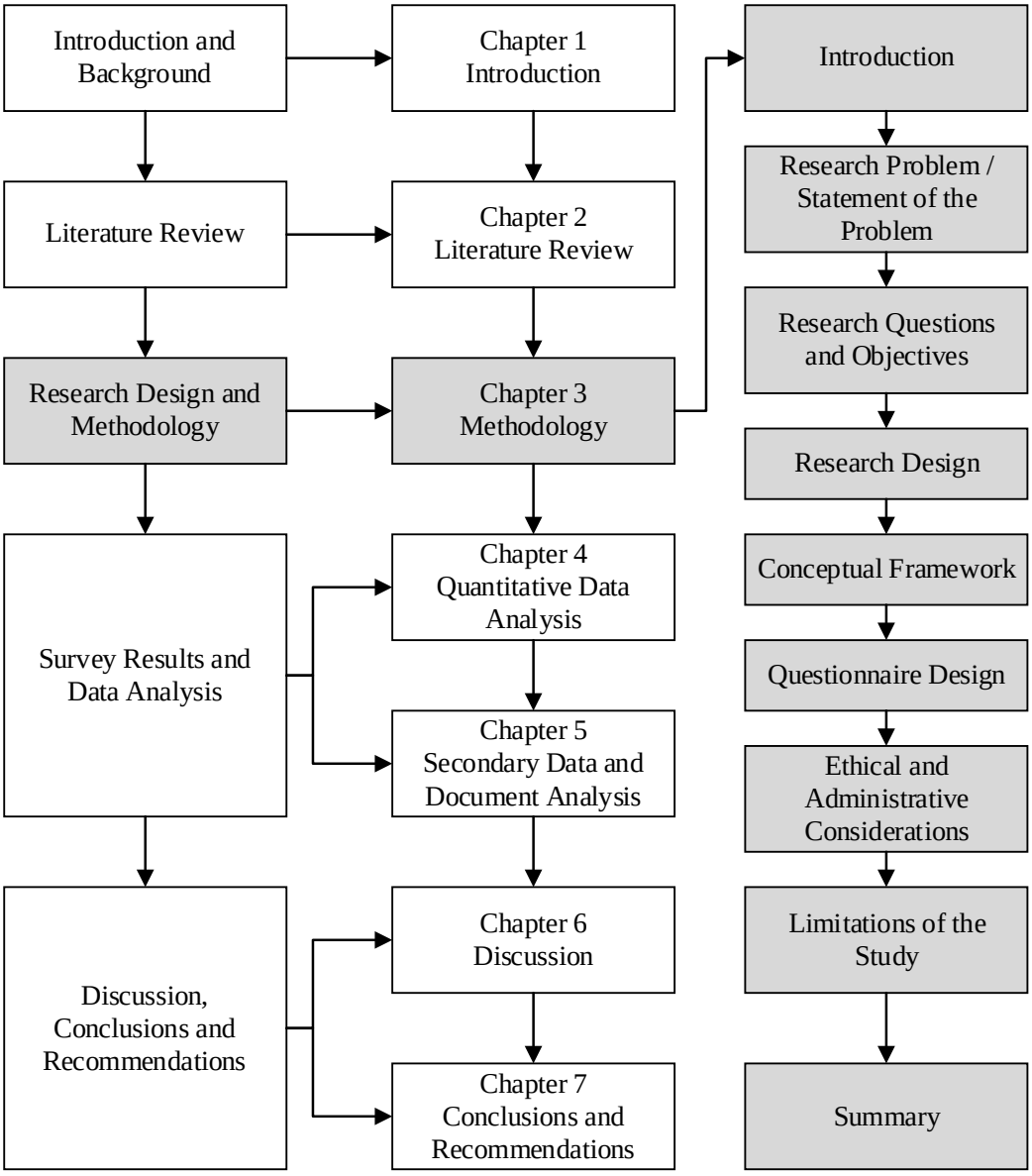


Figure 3-1: Graphical representation of Chapter 3 outline

3.2 Research Design

3.2.1 Research Approaches/Paradigms

The research philosophy used is a pragmatism paradigm using a cross-sectional case study with mixed methods. Pragmatism, as a paradigm, centres around the idea of employing optimal approaches to address practical issues in the real world (Teddlie & Tashakkori, 2006). This approach enables the incorporation of diverse information and knowledge to address research objectives effectively. Pragmatists are concerned with practical outcomes and solutions, valuing quantitative and qualitative data (Creswell, 2021). This philosophy fits the study as it is concerned with practical outcomes, such as developing a cybersecurity framework addressing factors influencing cybersecurity in the transportation sector of SA. It is also well-suited for mixed methods research and combined within a single study, in this case, the transport sector of SA, and focuses on what works in a given situation utilising various forms of quantitative and qualitative data.

The design elements utilised to perform this research are proposed in the 'Research Onion', represented in Section 3.2.2.

3.2.2 Research Onion

Researchers usually propose research to answer a question or address a problem. The researcher begins by determining what data are needed and then decides how they will obtain the data. Various techniques like questionnaires, observation and analysis can be used to obtain the data. The final decision about the overall research will only be represented by techniques used to obtain data and the methods to analyse these data (Saunders & Tosey, 2013). They used the representation of the 'Research Onion' to illustrate how the final design (the inner layer of the research onion) needed to be considered with other design elements (the outer layers of the research onion).

The 'Research Onion' is a metaphorical representation often used to illustrate the layers involved in the research process. It was introduced by Saunders, Lewis, and Thornhill (2009) in their research methods textbook. The layers of the onion represent different stages of the research, starting from the outer layer and moving inward. Each layer corresponds to a specific aspect or dimension that researchers must consider when designing and conducting a study.

The 'Research Onion' empowers researchers by guiding them in developing a comprehensive research design. As they peel through the layers, they can systematically address various elements of the research process. These layers typically include philosophy, approach, methodological choice, strategy, time horizon, data collection, and data analysis (Saunders, Lewis, Thornhill, & Bristow, 2015).

Using the 'Research Onion', researchers can ensure that their chosen methods align coherently with their philosophical stance and research objectives. It provides a structured approach, helping researchers make informed decisions at each layer. Consequently, it enhances the research design's transparency, rigour, and reliability, making it a valuable tool for planning and conducting studies. Readers benefit from understanding the 'Research Onion' as it clarifies the logical progression and rationale behind the chosen research methods, contributing to the overall credibility of the study (Saunders & Tosey, 2013).

Figure 3.2 represents the proposed 'Research Onion' and the different design elements used to conduct this research. Each layer is discussed in Section 3.2.2.

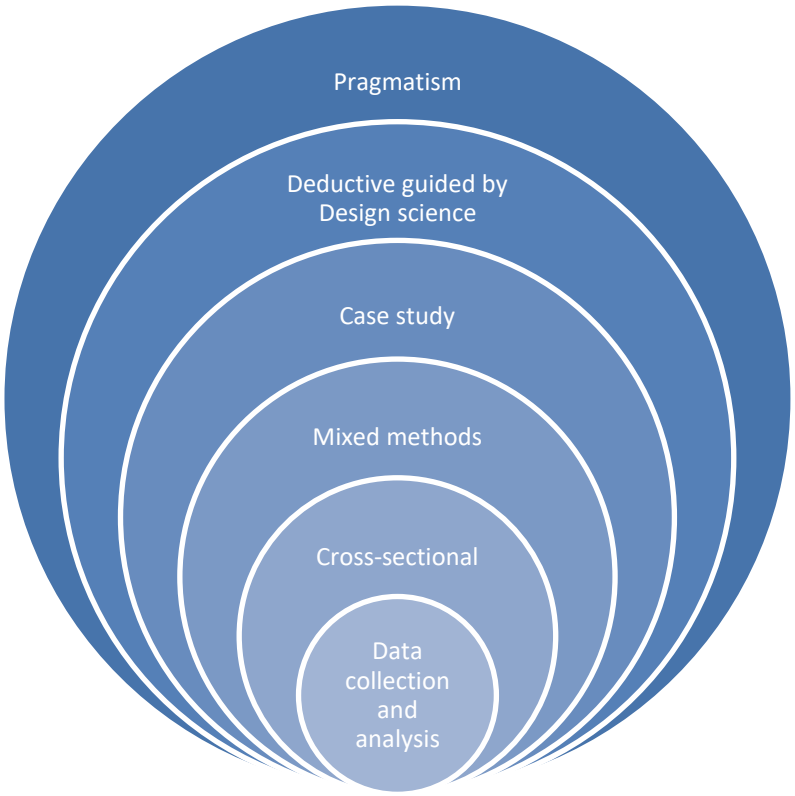


Figure 3-2: Research Onion for the Study

Adapted from: Saunders and Tosey, 2013

- **Philosophy** - The pragmatism philosophy represents the outer layer of the research onion. The pragmatism philosophy (Gunesh, 2016) is used as described in the Section 3.2 above.
- **Approach** - The study applied the deductive approach guided by Design Science Research. The deductive approach is used when the theoretical and conceptual structure is developed based on existing theory and then tested through observations. Design Science Research is an approach that merges scientific inquiry with the creation and assessment of innovative

artefacts or designs. It centres on solving real-world problems and generating practical knowledge and solutions (Peffers et al, 2006).

- **Methodological choice** – Two general categories of research methodologies are quantitative and qualitative. The first quantitative method provides numerical predictions, percentages, frequency, occurrence, trends, and others (Patton, 2005). In contrast, the qualitative method describes data in-depth, without data analysis or statistics and helps to understand how a person thinks or why an event occurs. The mixed methods approach is used. Mixed methods are when quantitative and qualitative methods are used for data gathering and analysis. The data gathered using quantitative methods, from participants with IIoT knowledge in the transport sector of SA, are used to determine the factors as per the research objectives in Section 1.5.2. The data gathered using the qualitative methods are used to triangulate as well as develop controls in the cybersecurity framework as discussed in Section 6.7.3. Data gathering and analysis for quantitative methods included questionnaires, document analysis and open-source tools. The qualitative data used included analysis of documents and white papers from leading advisories and publications including best practices, standards, and frameworks. A mixed-method approach is used to offset limitations that might exist in individual methods and to close any gaps in data.
- **Strategy** - The strategy used is a case study that will study a real-life instance's characteristics and a more realistic form of collecting data. Case studies are associated with qualitative and quantitative methods (Flick, 2009). This study is a singular case analysis conducted on the transportation sector of SA. It focuses on multiple organisations within the sector. Asomani-Boateng, Fricano and Adarkwa (2015) have used a case study to assess the socio-economic impact of rural road improvements in Ghana's transport sector, and Valderrama, Monroy and Behrentz (2019) have conducted a case study on the Colombian transport sector to determine the challenges of greenhouse gas mitigations. The purpose of the study is to conduct an in-depth analysis of the unique factors that influence IIoT cybersecurity in the transportation sector of SA. This will help develop and validate a cybersecurity framework. Case studies often use questionnaires to collect data. For example, Brazier, Cooke, and Moravan (2008) used questionnaires as part of their mixed-methods case study to evaluate the impact of a cancer care program and Crowe et al. (2011) in their research. This study used an online questionnaire to collect quantitative data, as discussed in Section 3.2.4.
- **Time horizon** - The next layer in the research onion is a cross-sectional study, which used mixed methods of research surveying and analysing data such as documents and whitepapers to measure the state of IIoT at a point in time. A cross-sectional study is used as the study is at a point in time, whereas a longitudinal study is over a period.

- **Data collection, and data analysis -** The choices of the sample groups and the questionnaires' context all form the research onion's inner layer. The outcomes of the questionnaires, data analysis and results contributed to the methodology to develop a cybersecurity framework and to validate the cybersecurity framework for relevance. Primary data is collected via a questionnaire which offered a highly efficient way of gathering large amounts of data to determine the factors of securing IIoT in the transportation sector of SA. Statistical-rich data is generated via this strategy. Various techniques from cybersecurity research will be used, including exploratory study, descriptive study, and security analytics (Edgar & Manz, 2017). General statistical techniques from security analytics are used (Talabis, McPherson, Miyamoto, & Martin, 2015).

3.2.3 Study Site

The study area is South Africa, focusing on several organisations and businesses in the transportation sector implementing IIoT and running ICS or SCADA systems, for example, logistics and transportation companies (public and private), public departments, municipalities, and professional bodies.

3.2.4 Data Collection Methods

Questionnaires were distributed electronically via email to the target population. Professional bodies (such as ISACA) were used to approach its members in the transportation sector. Closed-ended Likert scale questions align with the study's objectives; refer to Section 3.4 for the questionnaire design. Various documentary evidence is collected for the study. The sample for the document analysis is chosen by selecting common and freely available cybersecurity standards, frameworks and best practices related to Information security, IIoT and ICS/SCADA. The systematic approach to source, select and analyse these are further explained in Section 5.2.1. Data collected from the documents is analysed using tools such as NVivo. Open-source tools, such as Shodan, a search engine for internet-connected devices (including IIoT, IoT, ICS and SCADA), are used to collect data to determine the vulnerabilities of IIoT devices on the internet.

Table 3-1 sets out the different data collection methods and Figure 3.3 shows the quantitative and qualitative data collaboration.

Table 3-1: Data collection methods, Source: Author compiled

	Instrument	BMIS				Framework Development and validation	
		Technology	Organisation	Procedural	People	Development	Validation
Primary	Questionnaire	✓	✓	✓	✓	✓	
Secondary	Best practices, standards, and frameworks	✓	✓	✓	✓	✓	✓
	Shodan and other open-source tools	✓					
	MITRE ATT&CK						✓

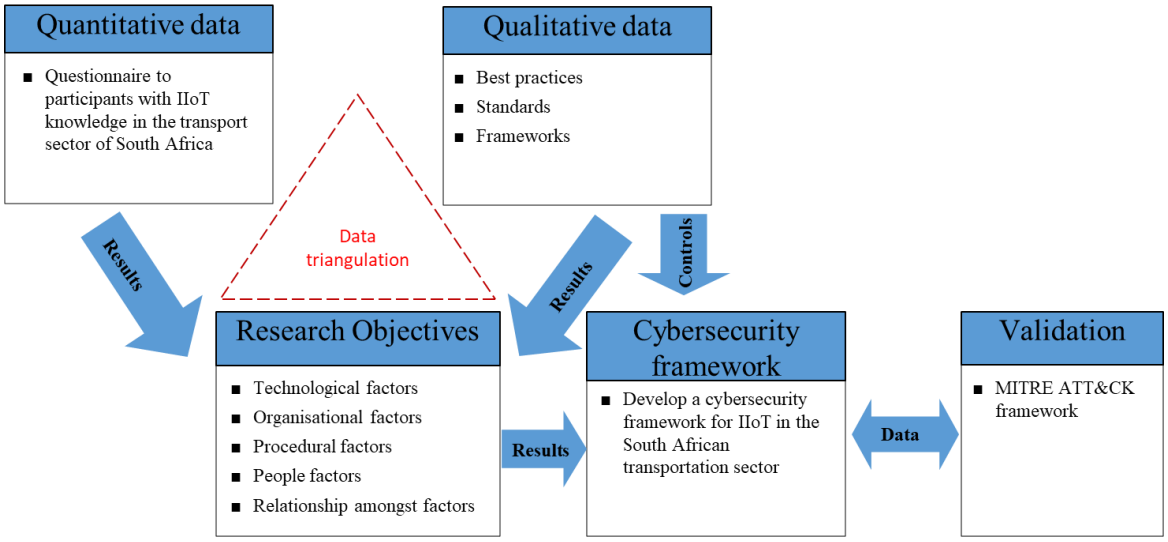


Figure 3-3: Quantitative and Qualitative Collaboration

3.2.5 Target Population

Professionals in the transportation sector with IT, Governance, Risk, Compliance, and Information Security knowledge, working with IIoT, are the target population. The intent is to focus on people with relevant IIoT and ICS or SCADA knowledge in the transportation sector to obtain appropriate and suitable information. There are various communities (IFIP Working Group 9.10, ISACA South Africa chapter, CISO Alliances) which was used to approach its members with the appropriate

professional knowledge in the transportation sector to partake in the questionnaires. The participants were from the transportation sector, Private Logistics companies, large State-Owned Company (SOC), as well as government departments which focus on the transport sector.

3.2.6 Sampling Strategies

A sample is a subset of the entire population from which data is obtained by the researcher (Yin, 2009). The sample of this study is selected from Information Security, Governance and SCADA/ICS professionals with experience with IIoT security. The questionnaire had a covering question to establish the relevance of the respondent.

As this is still a growing field in South Africa, there are expected to be limited people with knowledge and experience, and it is difficult to determine a precise population. Therefore, the sampling strategy used is convenience snowball, starting with a small set of the various communities and organisations with known deployments or knowledge of IIoT devices in the transportation sector. These include communities such as IFIP Working Group 9.10, ISACA South Africa chapter, CISO Alliances and companies as mentioned in the target population. These organisations are selected based on convenience of access. ISACA is the largest body of professionals with cybersecurity and IT governance knowledge in SA, and therefore, there is a higher chance of receiving valid responses. They also pointed to more relevant people and populations, which is expanded for the questionnaire. A convenient sample (non-probabilistic) is taken based on those who have worked on IIoT projects in the sector. The questionnaire is aimed at influential players. The sample for the document analysis is chosen by selecting common and freely available cybersecurity standards, frameworks and best practices related to Information security, IIoT and ICS/SCADA based on the IIoT relevance and percentage of responses from the questionnaires.

3.2.7 Sample and Sample Size

Due to the population uncertainty in the transportation sector, as discussed above, the questionnaire sample size consisted of at least 30 people involved in IIoT deployments. However, the total number of relevant participants with knowledge of IIoT security and transport sector were 58. These people are across several professional groups and organisations with knowledge of IIoT devices in the transportation sector, as mentioned above in the target population.

International best practices (IoT and IIoT standards and frameworks) are used for document analysis. The relevance and availability of the documents determine the sample size. These included reports by security vendors on security incidents, threats and vulnerabilities related to Industrial systems. Searches among relevant professional and technical organisations are conducted to identify relevant white papers, standards, and frameworks. Currently, five documents have been identified during initial literature searches.

This study selected a sample of professionals in Information Technology (IT), Engineering, Project Management, Governance, Risk, Compliance, and Information Security roles who have knowledge of IoT or IIoT security. A covering question in the questionnaire established the knowledge of the respondent.

3.2.8 Data Quality Control

Multiple methods are used for data quality control. The data triangulation of the multiple methods will complement the various methods and improve data quality.

Cronbach Alpha is used to show reliability and consistency from the responses received, refer to Section 4.8. Cronbach's alpha evaluates reliability by examining the extent of shared variance, or covariance, among the items comprising an instrument in comparison to the overall variance. The underlying concept is that a reliable instrument should exhibit a significant amount of covariance among its items relative to the total variance (Collins, 2007). Cronbach's alpha also assesses internal consistency, indicating the degree of interconnectedness among a set of items (Taber, 2017).

Closed-ended Likert scale questions are used in line with the study's objectives. A covering question is asked to determine the respondent's experience with IIoT systems and relevance to the transport sector. Questionnaires are designed to ensure that there are no missing or incomplete data by using the Google forms and mandatory answers.

External validity is gauging the accuracy of a study beyond the sample, determining its generalizability to other settings, populations, and measures (Dovetail Editorial Team, 2023). The primary data results obtained from questionnaires and document analysis used to develop the cybersecurity framework are compared against MITRE ATT&CK framework to ensure validity as shown in Figure 3-4.

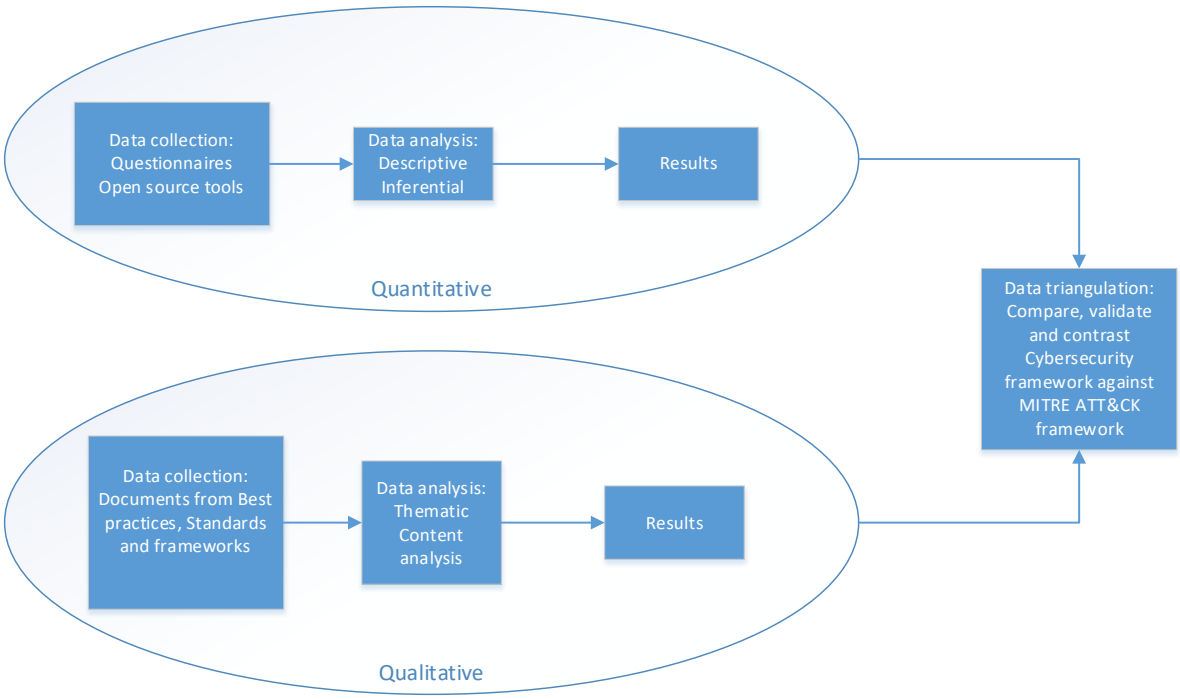


Figure 3-4: Research and data analysis methods

Source: Author compiled

3.2.9 Measurements

A mixture of different measures is used. Semantic differential to determine the factors influencing IIoT cybersecurity, and Likert, to scale responses from the questionnaires. Documents are measured using thematic analysis to determine the prevalence of themes and content analysis to determine key terms or phrases indicating sentiment and options regarding the concepts in question. Secondary data are analysed as explained in Section 3.2.10.

3.2.10 Data Analysis

According to Rubin (2008), data analysis is the art of analysing raw data to conclude the information. According to Bowen (2009), *document analysis* is the systematic procedure for evaluating or reviewing documents. Thematic analysis is used to identify themes within the data gathered from document analysis. This method is appropriate as this technique groups or associates the data gathered, and then the analysis is used to describe the data sets in full. Qualitative analysis software, such as NVivo 12 Pro, is used to analyse documents. This assisted in identifying trends and patterns as well as thematic analysis.

Statistics, such as descriptive statistics, correlation, and inferential statistics, describe the data obtained from questionnaires, Shodan and other open-source tools, best practices, standards, and frameworks. These methods summarised and described the data. Correlation and inferential statistics are used to determine the factors of the BMIS framework influencing IIoT security and relationships amongst the

BMIS variables. Tools such as Excel and NVivo perform the coding and summarising process. The coding is as follows: red if the techniques used by attackers are not mitigated by control/s in the cybersecurity framework, orange if control/s in the cybersecurity framework partially mitigate the techniques used by attackers, and green if control/s in the cybersecurity framework mitigated the techniques used by attackers.

Descriptive statistics are used to analyse the data to show patterns and summarise the data to determine the technological (threats, risks, and vulnerabilities), organisational, procedural and people factors to develop a cybersecurity framework for IIoT in the transport sector of SA. Cronbach Alpha is used to show reliability from the responses received. Due to the author's Honours Degree in Statistics, the author performs statistical analysis.

Correlation is used to determine the relationship between two variables. Where the correlation coefficient, *r*, is between example, -0.3 to -0.1, the correlation is weak. A strong correlation is when the correlation coefficient, *r*, is between -1 to -0.5 or 0.5 to 1 (MathBits, 2016).

Combining several data analysis methods allowed the data to be handled in a way that made it possible to interpret, validate and define the requirements to develop a control framework for IIoT deployment in the transport sector for SA.

3.3 Conceptual Framework

The study's primary research approach is centred on Design Science Research (DSR). The conceptual framework uses the Information Systems research framework and guidelines for DSR (discussed in Section 3.3.3) combined with BMIS. The framework development from Section 3.3.1 will be followed for the cybersecurity framework development based on the steps listed and input from BMIS, all guided by DSR.

3.3.1 Framework Development

The framework development process consisted of several steps. The overall environment needs to be understood, including threats, vulnerabilities, risk, the business environment, and the systems (CPNI 2008). The CPNI (2008) list the following steps in developing a framework: Understand the business risks → implement secure architecture → establish response capabilities → improve awareness and skills → manage third-party risk → engage projects → establish ongoing governance. To fully understand business risk, one must understand the risks, threats, vulnerabilities, organisation, processes, and people.

The process can also be grouped, as displayed in Figure 3.5.

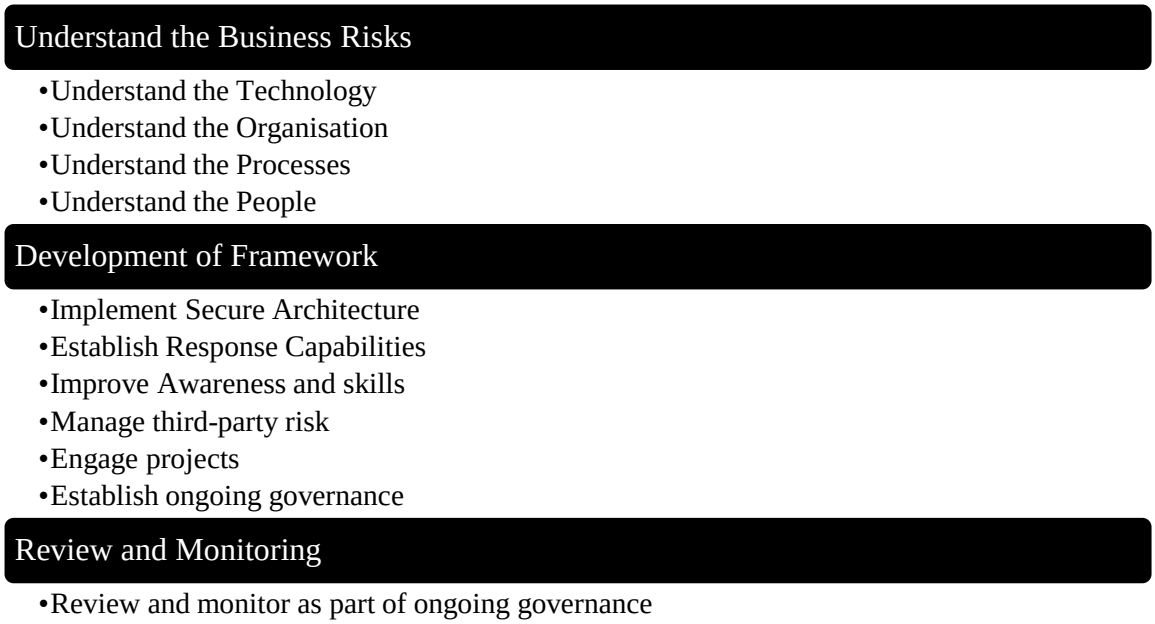


Figure 3-5: Framework development steps

Adapted from: CPNI (2008)

Before a control framework is developed, a company needs to understand the risk they face from likely compromises to IIoT systems. To comprehensively understand the business risk, an organisation should commence by understanding the People, Process and Technology (PPT) (Rodriguez & Edwards, 2010). The PPT application model for Information Systems risk management was applied to small/medium enterprises (SMEs) by (Muhammad & Iqbal, 2017). This was applied to SMEs but could also be applied to larger organisations. The type of organisation, i.e., size and structure, needs to be considered to determine risks to their environment. Therefore, understanding the business risks includes the organisation's understanding of People, Processes, Technology and Organisation; each of the steps from 'Understanding the business risks' needs to be conducted independently. The subsequent steps are integral to framework development and fall within its purview: Implement secure architecture, establish response capabilities, improve awareness and skills, manage third-party risk, engage projects, and establish ongoing governance. Considering the aspects mentioned earlier, these elements can be represented within a process or methodology for developing a control framework. The steps in the methodology are illustrated in Figure 3.6.

Figure 3-6: Framework Development Methodology

Adapted from: CPNI (2008)

3.3.1.1 Understand the People

The people component within an organisation refers to the human resources available for various tasks, often utilising technology. One crucial task is onboarding suitable individuals with the necessary skills, experience, and attitude. Providing clear role definitions to the people involved is equally essential, ensuring everyone understands their responsibilities (Khanduri, 2022). The people and skills required to support IIoT systems must be determined.

3.3.1.2 Understand the Process

The process component within an organisation encompasses a series of steps or actions undertaken to accomplish a specific objective. The processes primarily focus on the how aspect. They outline how the desired outcome will be achieved and how the available resources, including people and technology, will be utilised to address the business problem. Processes are designed to be replicable, consistently yielding the intended outcome regardless of the individual performing them (Khanduri, 2022). Processes for managing and supporting IIoT systems need to be evaluated.

3.3.1.3 Understand the Technology

Technology equips individuals with the necessary tools to execute the process and often aids in automating certain aspects. Organisations must exercise caution and ensure the chosen technology aligns with their specific needs and seamlessly fits their existing infrastructure. While new and attractive tools may be tempting, it is essential to prioritise compatibility and suitability for the

organisation's requirements. Technology also introduces new risks, threats and vulnerabilities to the organisation and needs to be fully understood (Khanduri, 2022). The threats, vulnerabilities, and risks to IIoT environment must be determined. Section 2.3.5 lists possible vulnerabilities, threats, and risks to IIoT systems.

3.3.1.4 Understand the Organisation

The organisational perspective encompasses the dimensions of size, structure, and management support. It plays a vital role in shaping strategy, processes, and culture design. The strategy should be flexible enough to adapt to external and internal factors, allowing the organisation to respond effectively to changing circumstances.

3.3.1.5 Development of Frameworks

A control framework is developed based on the business risk assessment, which includes the people, process, technology, and organisation elements of the IIoT environment. The framework should include technical, procedural and management controls to protect the IIoT systems adequately. The framework should also include the implementation of secure architecture, the establishment of response capabilities, improvement of awareness and skills, management of third-party risk, project management and establishment of ongoing governance CPNI (2008).

3.3.1.6 Review and Monitoring

It is essential to regularly review the above steps as any changes to systems, threats, impacts, or vulnerabilities will change the business risk and either render specific controls in the framework outdated or inadequate. For example, implementing new technology such as Artificial Intelligence (AI) brings new risks, threats and vulnerabilities to the organisation, and adequate mitigating controls must be implemented to cater for them. Ongoing environmental monitoring needs to occur to identify any new systems changes, threats, vulnerabilities, and corresponding updates of the control framework should occur at a minimum annually CPNI (2008).

3.3.2 Business Model for Information Security (BMIS)

The conceptual framework that will guide the study is the Business Model for Information Security (BMIS). ISACA developed the BMIS, previously the Information Systems Audit and Control Association. They are an international body with leading practices on standards, certifications, and knowledge (ISACA, 2023).

The BMIS emphasise the interrelationship of numerous processes and components. These are the technology, organisation and size, process, and people aspects of Information Security. This framework can be used by companies of all sizes (ISACA, 2010b). The processes and components of the BMIS are illustrated in Figure 3.7.

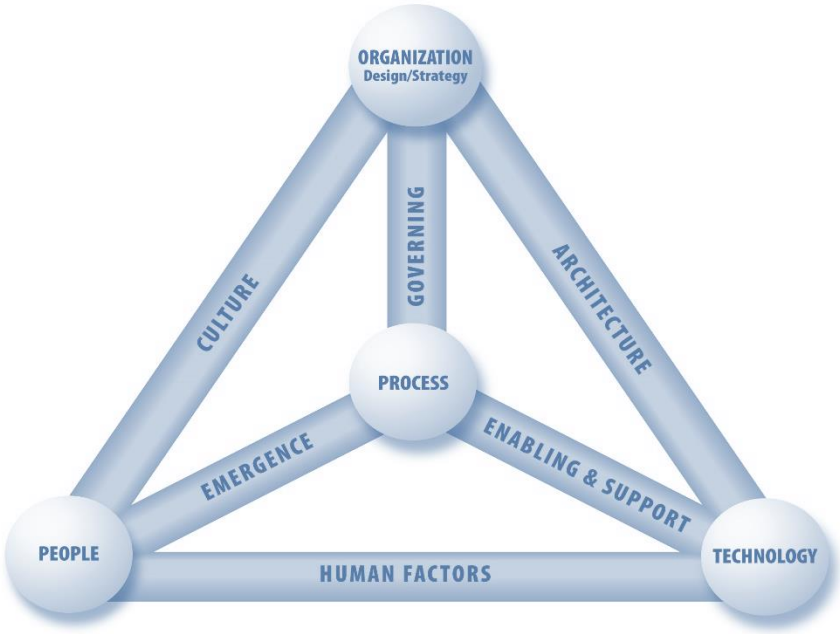


Figure 3-7: Business Model for Information Security (BMIS)

Source: ISACA (2010a: 13)

The four areas listed by the BMIS framework that influence adopting and implementing innovative or new technology from an organisation's perspective are the technological, organisational, people and environmental perspectives. When these four elements are combined, it forms the BMIS framework. Each aspect is briefly discussed below (ISACA, 2010a:13):

- Technological perspective refers to technologies from both an internal and external aspect relevant to or influencing the organisation. Given an organisation's dependence on technology, it establishes a vital part of the organisation's infrastructure and a critical component in accomplishing its strategy.
- The organisational perspective refers to the organisation's size, structure, and management support. Processes, culture, and strategy are essential to determine the design. The strategy should be flexible to adjust to both external and internal factors.
- Procedural perspective refers to the processes to identify, manage and control the risk, confidentiality, integrity, and availability. These originate from the strategy and control of the operational part of the organisation. These also include relationships with the government to comply with legal requirements.
- The people aspect denotes the human resources and the issues that come with them. It describes the accountability for each part of the strategy. The human element must consider behaviour, values, and support. It forms a critical part of any organisation.

The four areas of BMIS listed below guided the case study (ISACA, 2010a:13):

- Technology → there are new and existing threats due to IIoT that influence the organisation. IIoT also has vulnerabilities as well as technical security measures relevant to the organisation or influencing the organisation. The risk that IIoT has on the organisation when it is introduced.
- Organisational → the influence that IIoT has on the organisation will be determined by aspects such as the size, structure, Cybersecurity strategy, Risk appetite, Innovativeness and security culture, and senior executive management engagement with security.
- Procedural → the procedures under which the organisation operates will influence the cybersecurity of IIoT devices. Security incident response, risk management, IT governance and procedures, policies, standards, compliance, and regulatory requirements from the government (POPI, RICA, CAC, King IV, ECT Act) will have an influence.
- People → the human element always has a significant impact on an organisation. The following people factors will influence IIoT cybersecurity in the organisation: cybersecurity awareness, enablement, employee engagement and satisfaction.

The BMIS was chosen for this study due to its strong alignment with the research objectives outlined in Section 1.5.2, which encompass technology, organisational, procedural, and people-oriented aspects. This selection is motivated by the BMIS's comprehensive nature, which encompasses various dimensions, including business and technical elements, thereby offering a more holistic perspective of the study.

3.3.3 Design Science Research

Design Science Research (DSR) is an approach that merges scientific inquiry with creating and assessing innovative artefacts or designs. It centres on solving real-world problems and generating practical knowledge and solutions. Researchers in design science aim to develop new theories, frameworks, models, or systems that can be practically applied and tested. The research process involves iterative design, implementation, evaluation, and refinement cycles to produce artefacts that contribute to theoretical understanding and practical applications within a specific field. Design science research finds common application in disciplines such as information systems, engineering, and management, where the emphasis lies in creating effective and valuable solutions for complex challenges (Peffers et al., 2006). Peffers et al. (2006) lists six steps in Design Science research; they are listed below and displayed in Figure 3.8.

Step 1: Problem Identification and Motivation: Recognize and articulate the problem or opportunity driving the need for research. Gain a thorough understanding of the context, stakeholders, and objectives.

Step 2: Definition of objectives of a solution: Establish the objectives and goals the research intends to achieve. Formulate precise research questions or hypotheses.

Step 3: Design and Development: Generate and design inventive artefacts, such as models, frameworks, or systems, that can address the identified problem or opportunity. Develop these artefacts based on theoretical foundations and prior research.

Step 4: Demonstration: Demonstrate the operational and practical suitability of the designed artefacts through tangible prototypes or practical demonstrations. Present compelling evidence showcasing how the artefacts effectively address the identified problem or opportunity and verify their feasibility and effectiveness in real-world scenarios.

Step 5: Evaluation: Assess the effectiveness and utility of the artefacts through rigorous evaluation methods, including experiments, simulations, or case studies. Measure their performance against predefined criteria and metrics.

Step 6: Communication: Discuss research outcomes through scholarly publications, reports, or presentations. Share the artefacts, findings, and insights with the relevant research community and stakeholders. Iterate on the research process based on feedback and lessons learned.

These steps involve an iterative approach, often requiring multiple design, evaluation, and reflection cycles to refine and enhance the artefacts and research outcomes.

Figure 3-8: Design Science Research

Source: Peffers et al., 2006

Since Peffers et al. (2006) published DSR, there have been many adoptions and modifications. Offermann, Levina, Schönherr, & Bub (2009) has compared five processes, including Peffers et al. (2006), and categorized them into three common stages as displayed in Table 3.2 and below:

- Problem Identification.
- Solution Design, and
- Evaluation.

These processes share a stage-gate orientation, with distinct phases for definition, design, and evaluation. Offermann et al. (2009) envisions iterative cycles of these three phases, with subsequent refinements of the design. Offermann et al. (2009) indicated that if a process is defined in a way that

aligns with these three phases (typically through DSR), it can also be customized or tailored accordingly. The DSR for this research meets the three phases mentioned by Offermann et al. (2009) and are customised accordingly.

Table 3-2: Design Science Research phases introduced by Offermann et al. (2009)

Adopted from: Offermann et al. (2009)

Phase	Description
1. Problem Identification	Research Problem/Statement, refer to Section 1.3 The current state of IIoT in SA and the factors influencing IIoT security are not known as there are limited studies and research in this area. These include the technological, organisational, procedural and people factors influencing the cybersecurity of IIoT in the transport sector of SA. This research will identify and assess the degree of relationships amongst the factors influencing IIoT cybersecurity in the transport sector of SA to develop and validate a cybersecurity framework aligned with the SA transportation sector.
2. Solution Design	Design of a cybersecurity framework, refer to Section 6.7.3
3. Evaluation	Use MITRE ATT&CK framework for evaluation, refer to Section 6.7.4.

Hevner, March, Park, & Ram (2004) compared behavioural science with Design Science (DS) in their journal. They introduced a framework (Figure 3.9) for Information Systems research and outlined guidelines for Design Science Research (DSR) in Table 3.3. Hevner et al. (2004) assert that Information Systems (IS) research offers both rigor and relevance. On the rigor side, as depicted in Figure 3.9, researchers draw applicable knowledge from the knowledge base, including existing theories and frameworks. On the relevance side, the necessity for a new artifact emerges, as articulated by business needs in Figure 3.9. These business needs may arise from people, organisations, or technology within the environment. In the centre of Figure 3.9 are the activities associated with the development, construction, and evaluation of the new artifact. At the bottom of Figure 3.9, the contribution is twofold: returning to the environment in the form of an artifact with practical value and contributing rigorously as new knowledge.

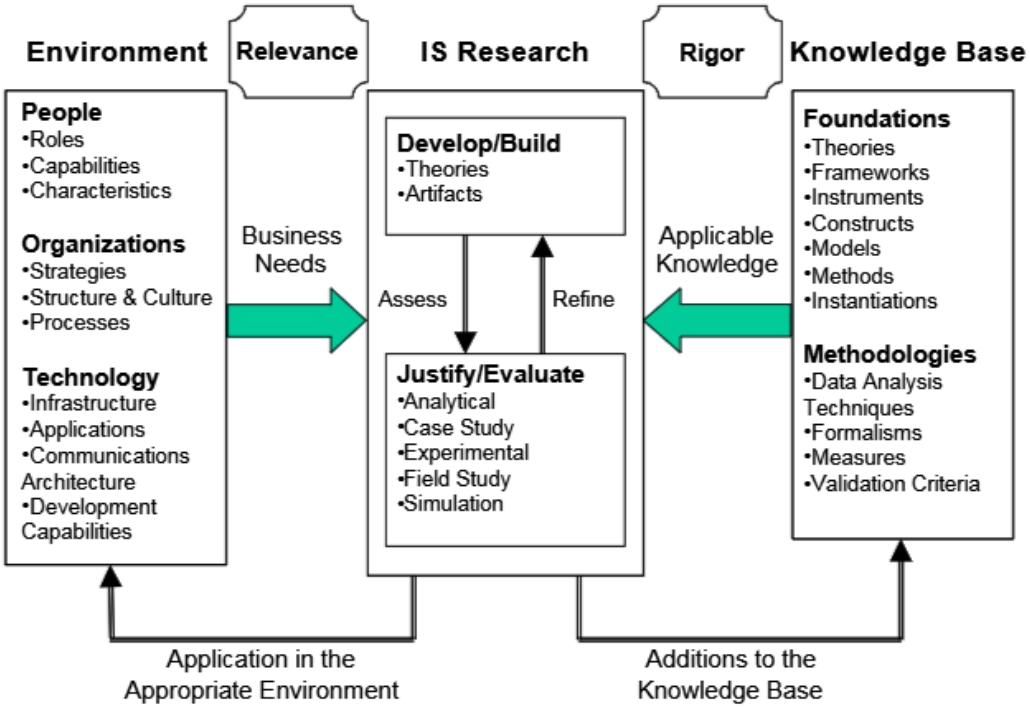


Figure 3-9: Information System Research Framework

Source: Hevner et al. (2004)

The seven guidelines for Design Science Research (DSR) outlined by Hevner et al. (2004), are summarised in Table 3.3.

Table 3-3: Design Science Research guidelines

Source: Hevner et al. (2004)

Guideline	Description
1. Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
2. Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
3. Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
4. Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, or design methodologies.
5. Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
6. Design as a Search Process	The search for an effective artifact requires utilising available means to reach desired ends while satisfying laws in the problem environment.
7. Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

The study will adopt the Information Systems research framework and guidelines for DSR from Hevner et al. (2004).

These guidelines involved in the study are populated with the outcome are listed in Table 3.4 below.

Table 3-4: Design Science Research guidelines used for the Study

Source: Author compiled, Adapted from: Hevner et al. (2004)

Guideline	Description
1. Design as an Artifact	Produced a viable artifact in the form of a cybersecurity framework, refer to Section 6.7.3
2. Problem Relevance	Research Problem/Statement, refer to Section 1.3 The current state of IIoT in SA and the factors influencing IIoT security are not known as there are limited studies and research in this area. These include the technological, organisational, procedural and people factors influencing the cybersecurity of IIoT in the transport sector of SA. This research will identify and assess the degree of relationships amongst the factors influencing IIoT cybersecurity in the transport sector of SA to develop and validate a cybersecurity framework aligned with the SA transportation sector.
3. Design Evaluation	Use MITRE ATT&CK framework for evaluation, refer to Section 6.7.4.
4. Research Contributions	Clear and verifiable contributions in the form of the cybersecurity framework as well as other contributions discussed in Section 1.8.
5. Research Rigor	Rigorous methods were used in the construction and evaluation of the design artifact refer Section 6.7. and Section 6.7.4.
6. Design as a Search Process	The search and design for an effective cybersecurity framework utilised available frameworks, standards, and best practices (refer to Section 5.2.1 and Section 6.7.3) to achieve the artifact while addressing the research objectives (Section 1.5.2).
7. Communication of Research	Communication of outcome in the thesis. Publication of outcome in journals, proceedings, and conferences, refer to Section 1.9.

The methodology of Design Science Research (DSR) which has been widely used in information systems research to address complex problems (Hevner et al., 2004; Kuechler & Vaishnavi, 2008; March & Smith, 1995; March & Storey, 2008) will be adopted for the conceptual framework directed by the seven guidelines and Information Systems framework by Hevner et al., 2004. This will be combined with BMIS as displayed in Figure 3.10 with each of the seven guidelines.

The following steps under **design and development**, are followed to conduct the case study, identify relationships, and develop a cybersecurity framework:

- Data selection and collection.
- Data analysis, coding and identifying relationships.
- Development of cybersecurity framework.
- Validate/verify and review.

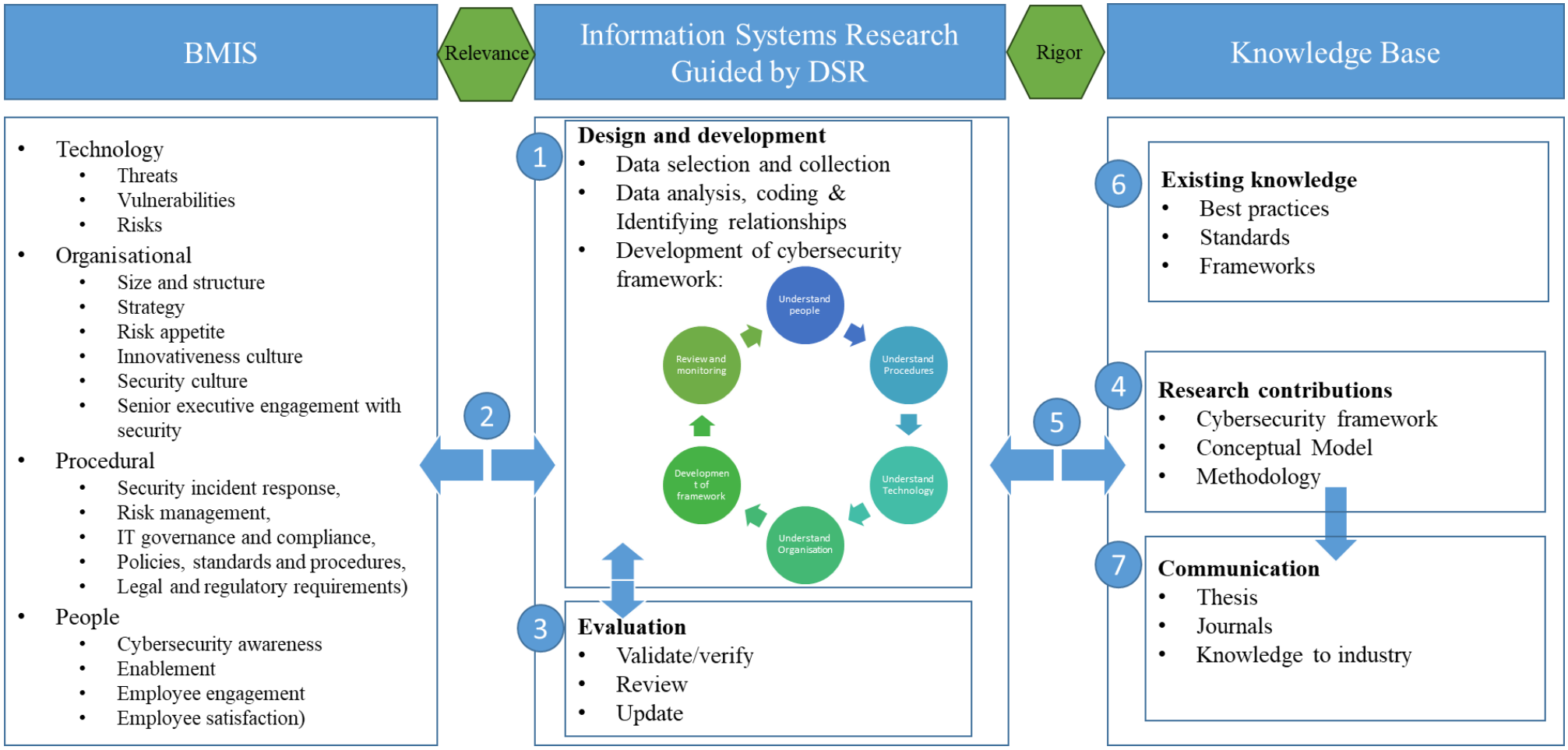


Figure 3-10: Conceptual Framework

Source: Adapted from Hevner et al. (2004)

3.4 Questionnaire Design

The questionnaire is one of the main research instruments. Closed-ended Likert scale questions are used in line with the study's objectives. A covering question is asked to determine the respondent's experience with IIoT systems. Those without knowledge of IIoT systems are further excluded from the study. Table 3.5 lists an outline of the questionnaire. The complete questionnaire can be found in Appendix A. Table 3.6 links the research objectives to the relevant questions.

Table 3-5: Outline of the questionnaire

Section	Details
Section A	Demographics
Section B	Technological Factors influencing IIoT
Section C	Organisational factors
Section D	Procedural factors
Section E	Human factors

Table 3-6: Research Objective linked to Questions

Research Objective	Question reference
RO1: To determine the extent to which the technological factors influence IIoT cybersecurity in the SA transportation sector: • Existing and new threats due to IIoT • Vulnerabilities • Risks	Section B
RO2: To critically assess the organisational factors influencing IIoT cybersecurity in the SA transportation sector: • Size and structure • Cybersecurity strategy • Risk appetite • Innovativeness culture • Security culture • Senior executive engagement with security	Section C
RO3: To critically assess the procedural factors influencing IIoT cybersecurity in the SA transportation sector: • Security incident response • Risk management • IT governance and compliance • Policies, standards, and procedures • Legal and regulatory requirements	Section D
RO4: To assess the extent of the people factors influencing IIoT cybersecurity in the SA transport sector: • Cybersecurity Awareness • Enablement • Employee engagement • Employee satisfaction	Section E

Research Objective	Question reference
RO5: To assess the degree of the relationships amongst the BMIS factors for IIoT cybersecurity in the SA transport sector.	N/A
RO6: To develop and validate a cybersecurity framework for IIoT in the SA transport sector using the data collected.	N/A

3.5 Ethical and Administrative Considerations

A research proposal was submitted to the Higher Degrees Committee of the School of Management, Information Technology and Governance at the University of KwaZulu-Natal. Comments and suggestions from the members are noted and incorporated. Refer to Appendix E for the ethical clearance letter.

The ethical clearance for this research was obtained from the University of KwaZulu-Natal and gatekeeper permissions from various organisations. These include a large State-Owned Company (SOC), which wished not to be named, a gatekeeper's letter from IFIP Working Group 9.10, a gatekeeper's letter from CISO Alliances and a gatekeeper's letter from ISACA South Africa. Gatekeeper's letters were obtained from any other organisation where the need arose. There was no impact on human dignity. Names are withheld to ensure confidentiality and integrity. Informed consent was obtained from respondents before participating in any of the questionnaires to allow them to choose whether to participate in the study based on their knowledge of the subject. The questionnaire responses are anonymous, and results are reported on aggregated data unrelated to the responder.

3.6 Summary

This chapter discussed the research problem and objectives, which is to identify and assess the factors and the degree of relationships among the factors influencing IIoT cybersecurity in the transport sector of SA to develop and validate a cybersecurity framework aligned with the SA transport sector. The research philosophy used is a pragmatism paradigm, with a deductive approach. A cross-sectional case study using mixed methods are discussed. The target population, sampling strategies, limitations, data collection, quality control and analysis are described. A conceptual framework, using Design Science Research approached, guided by BMIS is discussed as well as the methodology to develop a cybersecurity control framework for IIoT. The next chapter analyses the primary data (quantitative analysis) to determine the factors influencing IIoT in South Africa's transportation sector and as input to developing a cybersecurity framework.

Chapter 4 Quantitative Data Analysis

4.1 Introduction

In the previous chapter we formulated the methodologies and conceptual framework that will guide the study. This chapter presents an analysis of the quantitative data (online questionnaire), as described in Section 3.4. The results from this chapter (quantitative analysis) are used to determine the factors influencing IIoT in South Africa's transportation sector and as input to developing a cybersecurity framework. The results are also triangulated to the qualitative analysis in the next chapter.

The sample of this study is selected from professionals in IT, Governance, Risk, Compliance, and Information Security, as well as engineers and operational users working with IIoT in the transportation sector of South Africa. The intent is to specifically focus on people with relevant IIoT knowledge in the transportation sector of SA to obtain appropriate and suitable information. The online questionnaire is distributed via email to members of various communities (IFIP Working Group 9.10, CISO Alliances, ISACA South Africa chapter and a large SOC) to approach its members with the appropriate professional knowledge in the transportation sector.

One questionnaire was sent out to the professionals in the transportation sector with relevant knowledge of IIoT and the data was collected from October 2019 till April 2020 for a period of 6 months. The questionnaire asked a covering question to establish the respondent's relevance (experience with IIoT and to the transport sector) and attempts to address the research objectives as mentioned in Section 1.5.2. The number of responses received were 73, however 15 participants were excluded after the demographics section, as they either had no knowledge of IIoT or no experience in the transportation sector of South Africa. The total relevant participants were 58. The reliability tests in Section 4.8 show high internal consistency. Figure 4.1 is a graphical representation of the outline of this chapter and its overall structure. Previous versions of this section were published as an academic journal in the *Scientia Militaria: South African Journal of Military Studies* in 2023 (Pretorius & Van Niekerk, 2023)

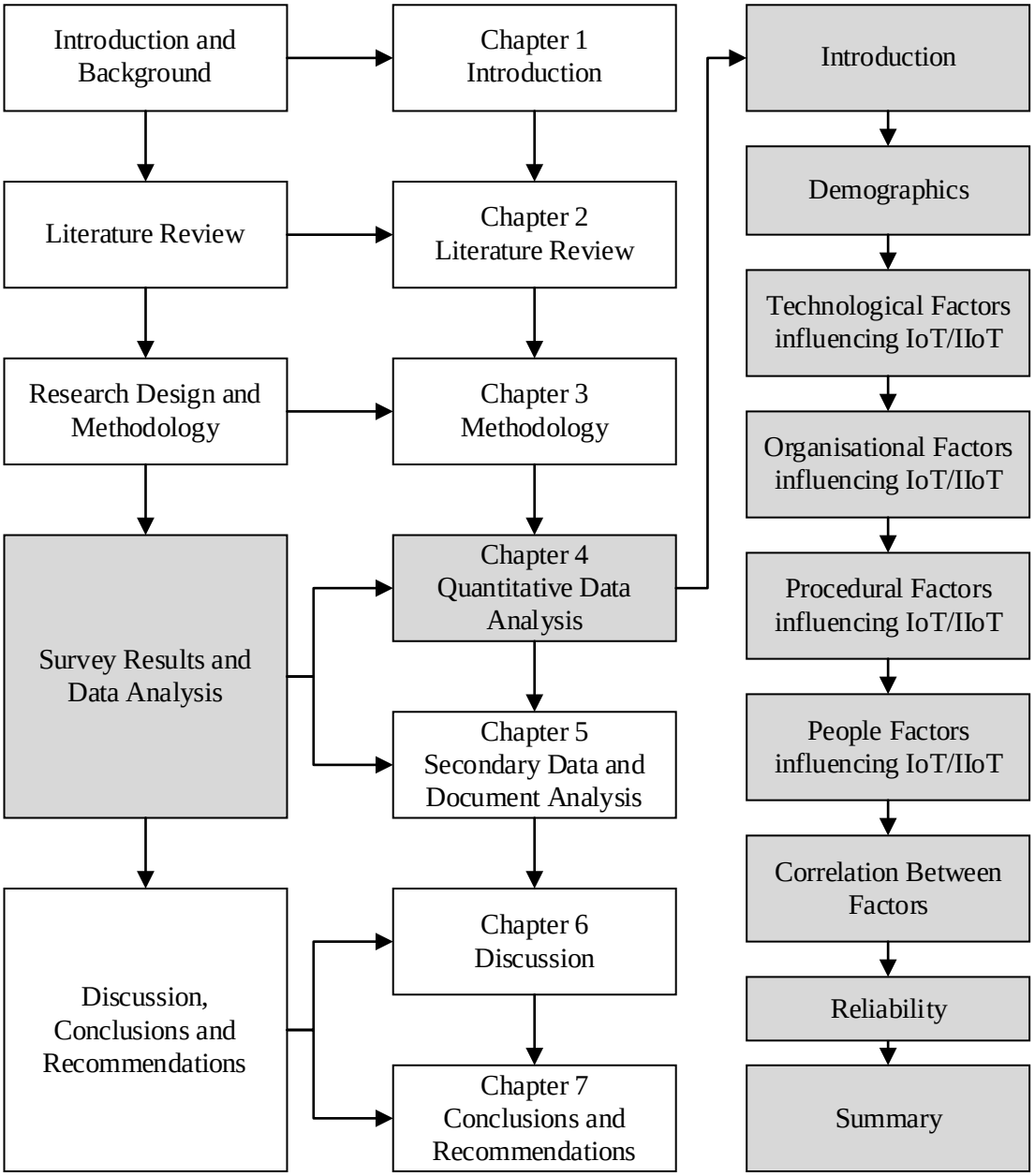


Figure 4-1: Graphical representation of Chapter 4 outline

4.2 Demographics

The Demographics relate to the following questions in the questionnaire:

- Question A1 Type of Organisation.
- Question A2 Job Function.
- Question A3 Number of Employees.
- Question A4 What is your primary interaction with IIoT.
- Question A5 How many years of experience with IIoT systems do you have? and
- Question A6 How many years of experience in the transport/logistics sector of South Africa?

4.2.1 Type of Organisation

A total of 73 responses were received from the participants. Those without IIoT experience and not relevant to the transportation sector of SA were excluded after the demographics. The total relevant participants were 58. Figure 4.2 illustrates the type of organisation to whom the respondents belong to. Most of the respondents (56 or 78%) are from a *Public Organisation*, 15 (21%) from a *Private Organisation*, and 1 (1%) from *Non-Governmental Organisation (NGO)/Non-profit organisation (NPO)*. The high response rate from public organisations was invaluable, as these entities manage majority of the critical infrastructure, significantly strengthening the research.

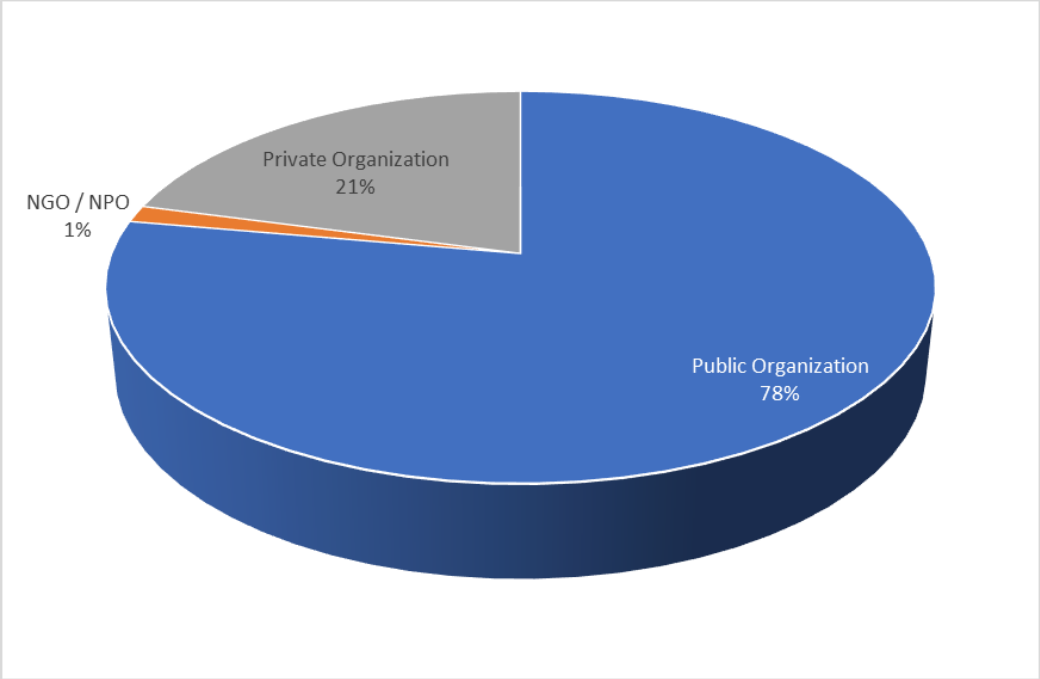


Figure 4-2: Type of organisations

4.2.2 Job Function

Figure 4.3 shows that 27 (37%) are in a management role, from which 16 (22%) of respondents are in a *Senior Management role*, and 11 (15%) are in a *Management role*. 12 (17%) of the respondents are in an *Analyst / Technical Role (IT / Information Security / Business etc.)*, 9 (12%) in an *IT Administrator* role (System / Network / Database administrator), 8 (11%) in a *C-level (CIO, CISO, CEO, CFO)* position, and 8 (11%) in a *Risk/Governance/Compliance role*. Both roles had 2 (3%), *Engineering* and *Human Resources*. The remaining participants comprised various roles at 1 (2%) from *Consultant*, *Developer*, *ICT Enterprise Architecture*, *Operations* and *Young Professional*. The split amongst the various job functions is suitable as the participants interact differently with IIoT based on their job function and will give a more accurate result.

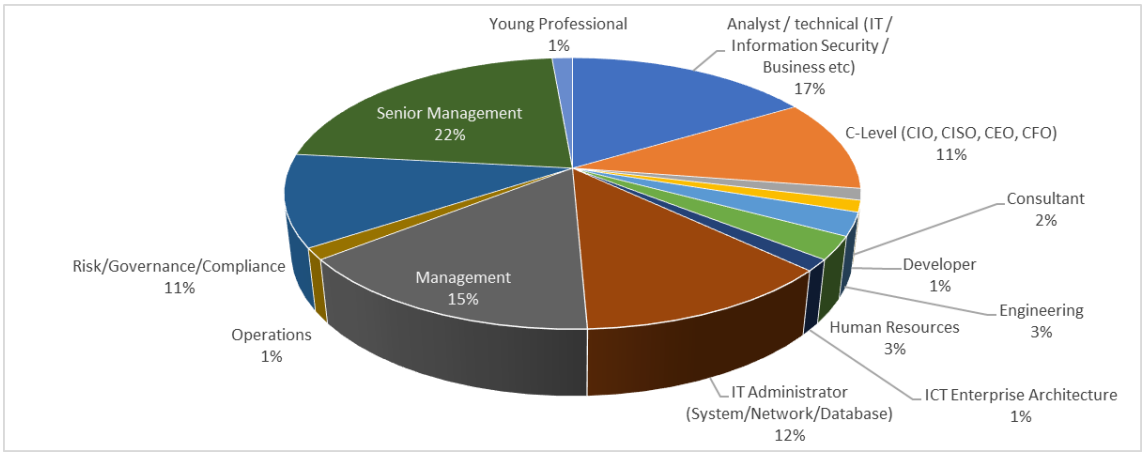


Figure 4-3: Job Function

4.2.3 Number of Employees

Figure 4.4 indicates that 51 (70%) of respondents work at a company with *5,000 or more* employees, 8 (11%) at a company with between *1,001 to 5,000* employees, 6 (8%) at a company with *100 – 1,000* employees and 8 (11%) at a company with *less than 100* employees. The results make sense as one of the communities that the questionnaire is sent to is a large SOC.

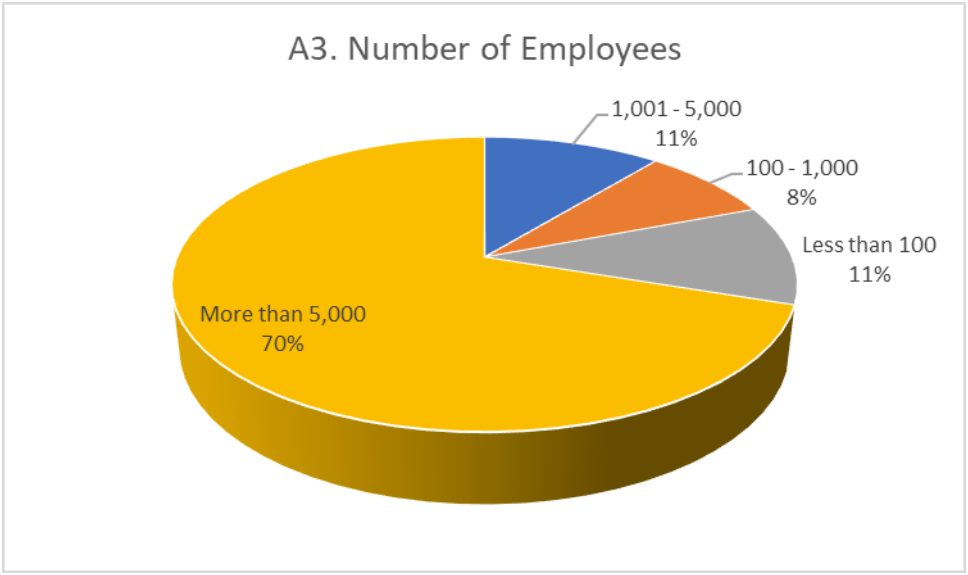


Figure 4-4: Number of employees (%)

4.2.4 Primary Interaction with IIoT

Figure 4.5 indicates that 8 (11%) of respondents had *No knowledge of IIoT*, 25 (34%) interacted with IIoT through *IT*, 12 (16%) via *Security*, 11 (15%) through *Governance / Risk / Compliance*, 7 (10%) through *Engineering / Operations / OT*, and 12% split between *Audit / Consulting* 4 (6%) and *Some*

awareness of the risks/issues 4 (6%). Of the remaining respondents, 1 (1%) interacted with IIoT via *Academic research* and *other* in the form of Medical Protocol Monitoring 1 (1%).

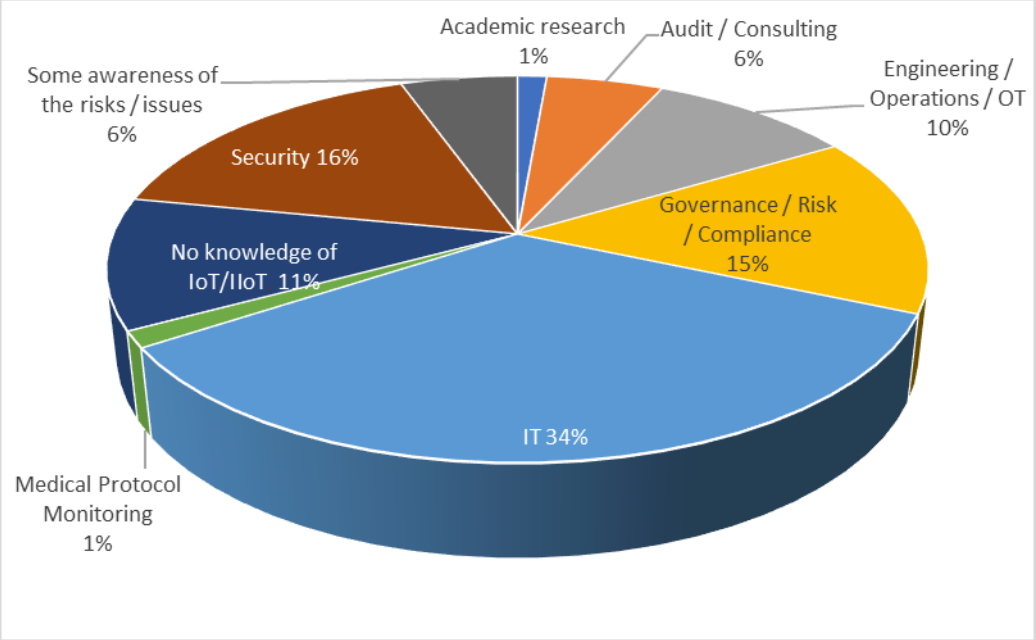


Figure 4-5: Primary interaction with IIoT

4.2.5 Experience with IIoT

Figure 4.6 depicts the respondents' years of IIoT experience. 52% (38) is split between *2 to 5 years*, 19 (26%) and *Less than 1 year* 19 (26%), 12 (16%) have *1 to 2 years* experience, while 8 (11%) have *None*. 7 (10%) of respondents have *5 to 10 years* of IIoT experience, 6 (8%) *10 to 20 years* and only 2 (3%) *more than 20 years*.

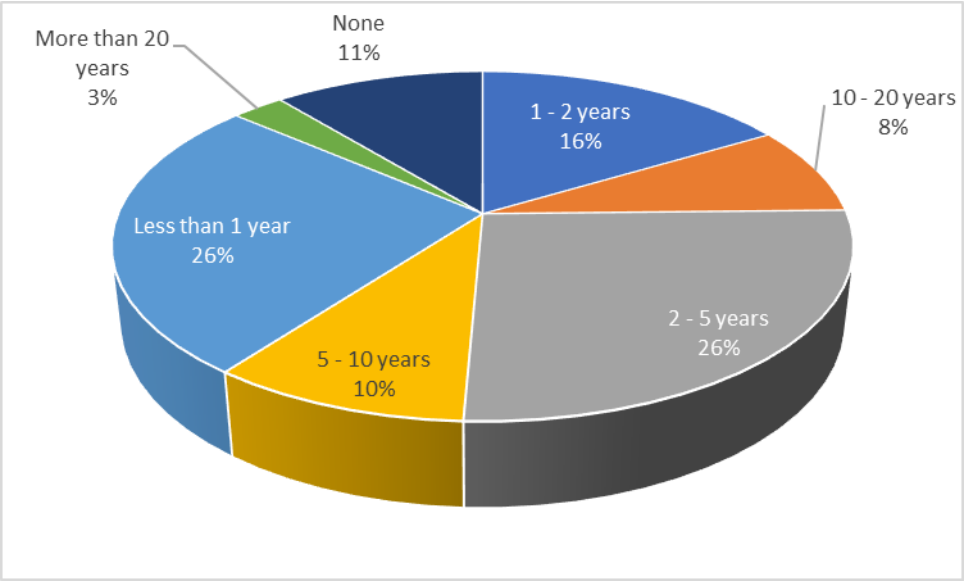


Figure 4-6: Experience with IIoT

4.2.6 Experience in the Transport Sector of South Africa

Figure 4.7 depicts the number of years of experience the respondents have in the transport/logistics sector in South Africa. 18 (25) have *5 to 10 years* of experience, 14 (19%) have *10 to 20 years*, and 12 (16%) have *more than 20 years* of experience in the transport/logistics sector in South Africa. 11 or 15% have *2 to 5 years* experience while 10 or 14% have no experience at all. The remaining 10 (11%) of respondents are split equally between those with experience in the transport/logistics sector of South Africa, with 5 (5.5%) having *1 to 2 years* of experience and 4 (5.5%) having *Less than 1 year*' experience.

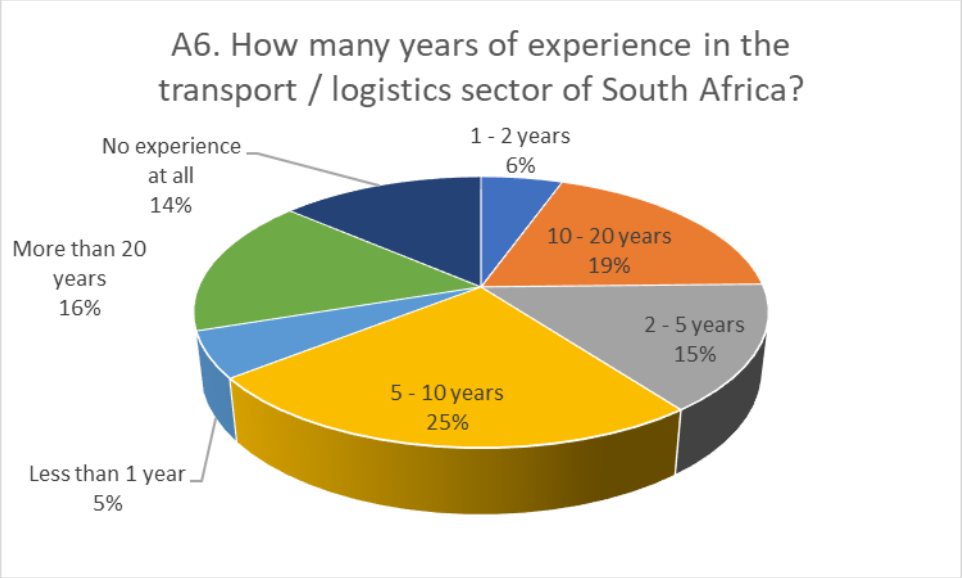


Figure 4-7: Experience in the transport/logistics sector in SA

After this question, the 8 (11%) participants that had no knowledge of IIoT as well as those with no experience in the transport / logistics sector of SA were excluded from answering further questions. A summary of the respondents is listed in Table 4.1.

4.3 Technological Factors Influencing IIoT

This section relates to the research objective to determine the Technological factors influencing IIoT security in the transportation sector of South Africa.

The responses received from the respondents for demographics in Section 4.2 included respondents with no knowledge of IIoT systems and no experience in the transportation sector of South Africa. The respondents with no knowledge of IIoT are excluded from this point. A total of 58 relevant

responses were included in the study. A summary of the respondent's knowledge of IIoT and the transport sector of SA is listed in Table 4.1.

Table 4-1: Summary of respondent's knowledge of IIoT

Respondent	Number of respondents	Result
No knowledge of IIoT or no experience in the transportation sector of South Africa	15 (21%)	Excluded from study
Knowledge of both IIoT and experience in the transportation sector of South Africa	58 (79%)	Included as relevant to study
Total	**73**	

4.3.1 Existing and New Threats Introduced by IIoT

The respondents are asked how they would rate the level of threats (new or existing) that IIoT would introduce in the transport sector of SA. This relates to Question B1 of the questionnaire. Figure 4.8 shows the existing and new threats introduced by IIoT in the SA transport sector. To generate the descriptive statistics, the responses are rated from '1', *No threat or not relevant*, '2' *No change in threats*, '3' *Slight increase in existing threats*, '4' as *IIoT increases existing threats* and '5' *IIoT introduces new threats*. Table 4.2 shows the frequency and full descriptive statistics of the threats (new or existing) that IIoT would introduce in the transport sector of SA, rating from *No threat or not relevant* to *IIoT introduces new threats*.

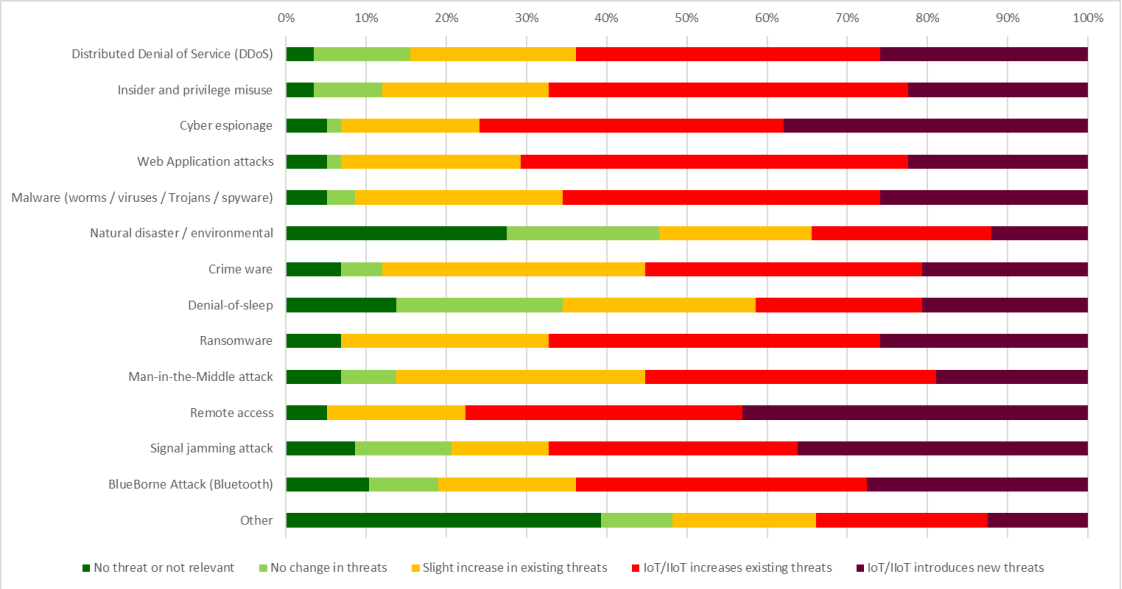


Figure 4-8: Existing and new threats introduced by IIoT

From the responses, it is noted that the top three threats (existing and new) likely to be introduced by IIoT in the transportation sector of SA are *Remote Access* with a mean of 4.1 (*IIoT increases existing threats*), *Cyber espionage* with a mean of 4.0 (*IIoT increases existing threats*) and *Ransomware* with a mean of 3.8 (leaning towards *IIoT increases existing threats*).

Table 4-2: Frequency and descriptive statistics table of threats

	DDoS	Insider and privilege misuse	Cyber espionage	Web Application attacks	Malware	Natural disaster / environmental	Crime ware	Denial-of-sleep	Ransomware	Man-in-the-Middle attack	Remote access	Signal jamming attack	BlueBorne Attack (Bluetooth)	Other
No threat or not relevant	2	2	3	3	3	16	4	8	4	4	3	5	6	22
No change in threats	7	5	1	1	2	11	3	12	0	4	0	7	5	5
Slight increase in existing threats	12	12	10	13	15	11	19	14	15	18	10	7	10	10
IIoT increases existing threats	22	26	22	28	23	13	20	12	24	21	20	18	21	12
IIoT introduces new threats	15	13	22	13	15	7	12	12	15	11	25	21	16	7
Mean	3.7	3.7	4.0	3.8	3.8	2.7	3.6	3.1	3.8	3.5	4.1	3.7	3.6	2.6
Median	4.0	4.0	4.0	4.0	4.0	3.0	4.0	3.0	4.0	4.0	4.0	4.0	4.0	3.0
Mode	4.0	4.0	4.0	4.0	4.0	1.0	4.0	3.0	4.0	4.0	5.0	5.0	4.0	1.0
Std Deviation	1.1	1.0	1.1	1.0	1.0	1.4	1.1	1.3	1.1	1.1	1.0	1.3	1.3	1.5
Variance	1.2	1.0	1.1	1.0	1.1	2.0	1.2	1.8	1.1	1.2	1.1	1.7	1.6	2.2
Kurtosis	-0.3	0.4	1.6	1.7	0.7	-1.3	0.2	-1.1	1.3	0.1	2.0	-0.5	-0.3	-1.5
Skewness	-0.6	-0.8	-1.3	-1.1	-0.9	0.2	-0.6	-0.1	-1.1	-0.6	-1.4	-0.8	-0.8	0.2
Confidence Level (95.0%)	0.3	0.3	0.3	0.3	0.3	0.4	0.3	0.4	0.3	0.3	0.3	0.3	0.3	0.4
Rank (Top)			2						3		1			
Rank (Bottom)						2		3						1

In statistics, a confidence interval is an estimate of the range of values in which the actual value of a population parameter is likely to fall with a certain degree of probability. Analysts usually use two levels of confidence - 95% or 99%. For instance, if a statistical model generates a point estimate of 10.00 with a 95% confidence interval of 9.50-10.50, it means there is a 95% chance that the actual value of the population parameter is somewhere between 9.50 and 10.50 (Hayes, 2023). This test is used to estimate the range in which the mean for the transportation sector population falls, given the sample mean and confidence intervals.

The 95% confidence intervals for the top three threats (existing and new) likely to be introduced by IIoT in the transportation sector in SA are all 0.3 for *Remote Access*, *Cyber Espionage*, and *Ransomware*. This indicates that with a 95% confidence, the population mean for each of the above is *Remote Access* with a population mean of between 3.8 (mean – confidence = 4.1 – 0.30) to 4.4 (mean + confidence = 4.1 + 0.30), *Cyber espionage* with a population mean of between 3.1 to 4.1and *Ransomware* with a population mean of 3.5 to 3.9.

The bottom three threats likely to occur are: *Other,* with a mean of 2.6, *Natural disasters / environmental,* with a mean of 2.7 and *Denial-of-sleep,* with a mean of 3.1, all leaning towards a *Slight increase in existing threats*. The category *Other* include disruptions caused by no maintenance, cyber warfare, defence evasion of existing security layers using IIoT, resistance to change (when IIoT creates more visibility), impact of the workforce (job losses, decrease in remuneration), and false positives that renders the benefits of IIoT sub-optimal.

When looking at the mode or the number of responses that appears most frequently, we see that *Remote Access* and *Signal Jamming attack* both have a mode of 5, indicating that the most frequent response selected is *IIoT introduces new threats*. Most of the threats (*DDoS*, *Insider and privilege misuse*, *Cyber espionage*, *Web Application attacks*, *Malware*, *Crime ware*, *Ransomware*, *Man-in-the-Middle attack*, and *BlueBorne Attacks (Bluetooth)*) have a mode of 4 (*IIoT increases existing threats*). The threat, *Denial-of-sleep,* has a mode of 3, indicating that the most frequent response selected is that IIoT introduces a *Slight increase in existing threats.* The remaining threats, namely *Natural disaster / environmental* and *other,* both have a mode of 1, indicating the most frequent response selected is that IIoT introduces *no threat or not relevant.*

Section 6.2.1 discusses the results further, including a unique analysis of the implications for the transport sector.

4.3.2 Top Threats

This relates to Question B2 of the questionnaire. The respondents are asked to indicate the top three threats by selecting only three on the question list. The top three threats are combined first, Malware (worms/viruses/Trojans/spyware) and Insider and privilege misuse, which was selected by 29 of the

respondents, and second Distributed Denial of Service (DDoS) with 26, and the third is Cyber espionage, with 25. The results are displayed in Figure 4.9.

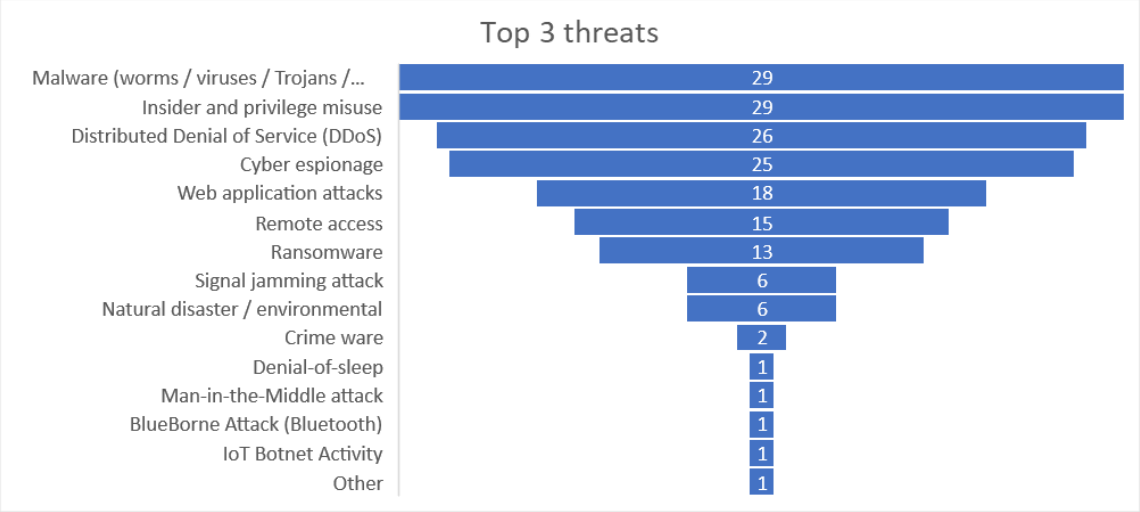


Figure 4-9: Top 3 threats related to IIoT

Comparing the top three threats with the top three threats that IIoT introduces in Section 4.3.2, it is observed that two of the top three threats correspond with the previous question (threats introduced by IIoT). The top threat of *Malware (worms/viruses/Trojans/spyware)* relates to the *Ransomware* threat likely to be introduced by IIoT and *Cyber espionage* as both the top threat and threat likely to be introduced by IIoT. Section 6.2.1 discusses the results further, including a unique analysis of the implications for the transport sector.

4.3.3 Vulnerabilities related to IIoT

This relates to Question B3 of the questionnaire. Figure 4.10 shows the vulnerabilities related to the IIoT environment in the transportation sector of South Africa. Table 4.3 shows the frequency of the vulnerabilities from *Very low* to *Very high* impact. To generate the descriptive statistics, the responses are rated from '1', *Very low impact*, to '5', *Very High impact*.

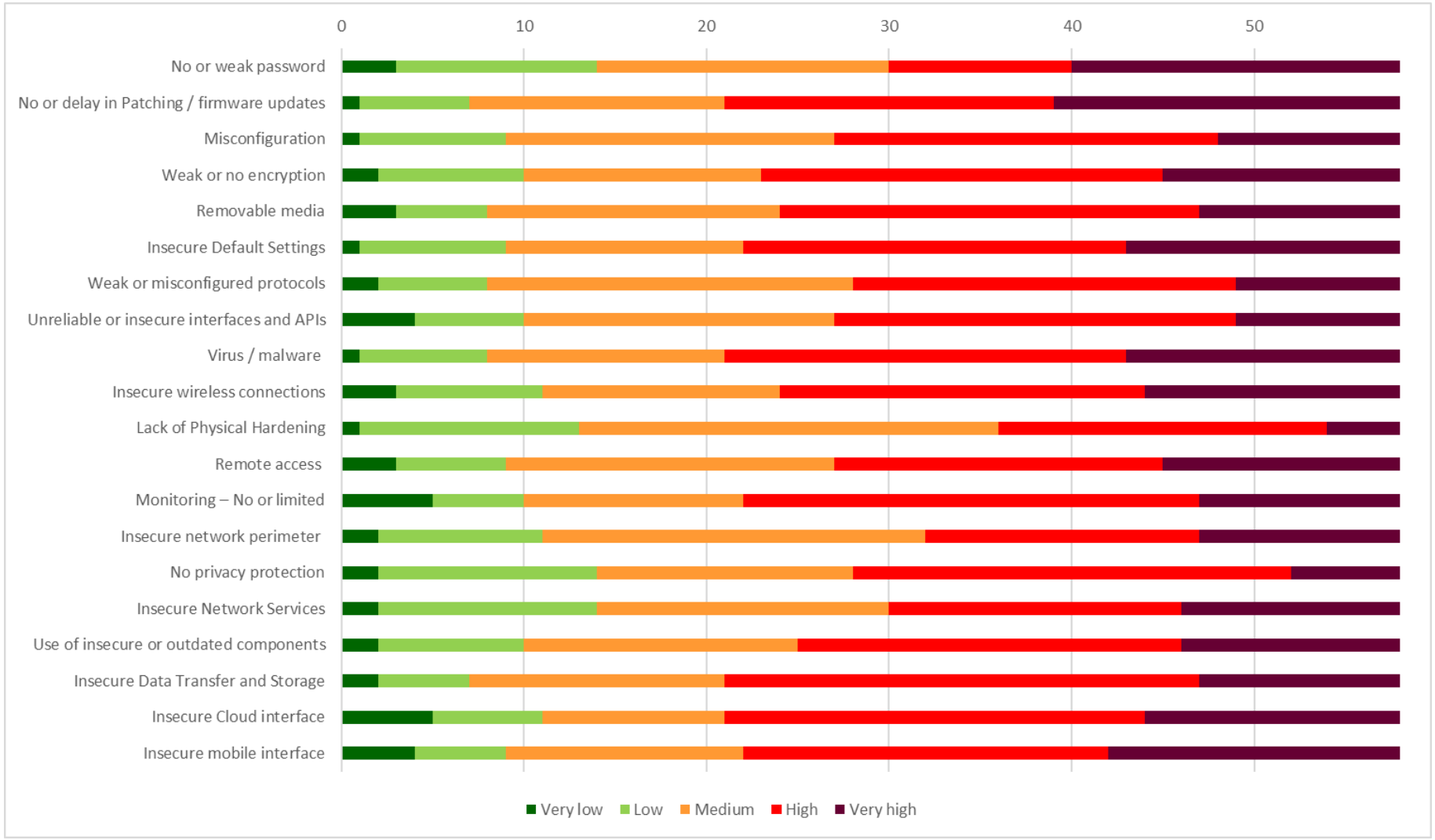


Figure 4-10: Vulnerabilities related to IIoT

From the responses, the top three vulnerabilities related to IIoT environment in the transportation sector of SA are *No or delay in Patching/firmware updates* with a mean of 3.8 (*Medium*, but leaning strongly towards *High*), combined second *Virus / malware (No software installed/unused/outdated), Insecure Default Settings*, *Insecure Data Transfer and Storage* and *Insecure mobile interface* all with a mean of 3.7 (also *Medium* and leaning towards *High*).

The 95% confidence intervals for the top three vulnerabilities are 0.30. This indicates that with 95% confidence, the population mean for each of the above is *No or delay in Patching/firmware updates* with a population mean of between 3.5 (mean – confidence = 3.8 – 0.30) to 4.1 (mean + confidence = 3.8 + 0.30), and *Virus / malware (No software installed/unused/outdated), Insecure Default Settings, Insecure Data Transfer and Storage* and *Insecure mobile interface* all with a population mean of 3.4 to 4.0.

Table 4-3: Frequency and descriptive statistics of the vulnerabilities

	No or weak password	**No or delay in Patching / firmware updates**	**Misconfiguration**	**Weak or no encryption**	**Removable media**	**Insecure Default Settings**	**Weak or misconfigured protocols**	**Unreliable or insecure interfaces and APIs**	**Virus / malware (No software installed/unused/outdated)**	**Insecure wireless connections (overlooked and poorly configured)**
Very low	3	1	1	2	3	1	2	4	1	3
Low	11	6	8	8	5	8	6	6	7	8
Medium	16	14	18	13	16	13	20	17	13	13
High	10	18	21	22	23	21	21	22	22	20
Very high	18	19	10	13	11	15	9	9	15	14
Mean	3.5	3.8	3.5	3.6	3.6	3.7	3.5	3.4	3.7	3.6
Median	3.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0
Mode	5.0	5.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0
Std Deviation	1.3	1.1	1.0	1.1	1.1	1.1	1.0	1.1	1.0	1.2
Variance	1.6	1.1	1.0	1.2	1.1	1.1	1.0	1.2	1.1	1.3
Kurtosis	-1.1	-0.5	-0.5	-0.4	0.1	-0.6	-0.1	-0.1	-0.4	-0.5
Skewness	-0.2	-0.6	-0.3	-0.5	-0.6	-0.5	-0.4	-0.6	-0.5	-0.5
Confidence Level (95.0%)	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3
Rank (Top)		1				2			2	
Rank (Bottom)								3		

	Lack of Physical Hardening	Remote access – authentication not secure / shared passwords for vendors	Monitoring – No or limited	Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)	No privacy protection	Insecure Network Services	Use of insecure or outdated components	Insecure Data Transfer and Storage	Insecure Cloud interface	Insecure mobile interface
Very low	1	3	5	2	2	2	2	2	5	4
Low	12	6	5	9	12	12	8	5	6	5
Medium	23	18	12	21	14	16	15	14	10	13
High	18	18	25	15	24	16	21	26	23	20
Very high	4	13	11	11	6	12	12	11	14	16
Mean	3.2	3.6	3.6	3.4	3.3	3.4	3.6	3.7	3.6	3.7
Median	3.0	4.0	4.0	3.0	4.0	3.0	4.0	4.0	4.0	4.0
Mode	3.0	4.0	4.0	3.0	4.0	4.0	4.0	4.0	4.0	4.0
Std Deviation	0.9	1.1	1.2	1.1	1.0	1.1	1.1	1.0	1.2	1.2
Variance	0.8	1.2	1.3	1.2	1.1	1.3	1.2	1.0	1.5	1.4
Kurtosis	-0.4	-0.3	0.0	-0.6	-0.6	-0.9	-0.4	0.3	-0.2	-0.1
Skewness	0.0	-0.5	-0.8	-0.1	-0.4	-0.1	-0.4	-0.7	-0.8	-0.7
Confidence Level (95.0%)	0.2	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3
Rank (Top)								2		2
Rank (Bottom)	1			3	2	3				

The bottom three vulnerabilities related to IIoT environment in the transportation sector of South Africa: *Lack of Physical Hardening* with a mean of 3.2, *No privacy protection* with a mean of 3.3 and third combined with a mean of 3.4, *Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)* and use of *insecure network services.*

Section 6.2.2 discusses the results further, including a unique analysis of the implications for the transport sector.

4.3.4 Risks of Unsecured IIoT (impact)

This relates to Question B4 of the questionnaire. Figure 4.11 shows the impact of the risks of unsecured IIoT devices in the transportation sector of South Africa. Table 4.4 shows the Risk Impact rating frequency and full descriptive statistics from *Insignificant* to *Extreme/Catastrophic*.

To generate the descriptive statistics, the responses are rated from '1', *Insignificant*, '2' *Minor*, '3' *Moderate*, '4' *Major* and '5', *Extreme/Catastrophic*.

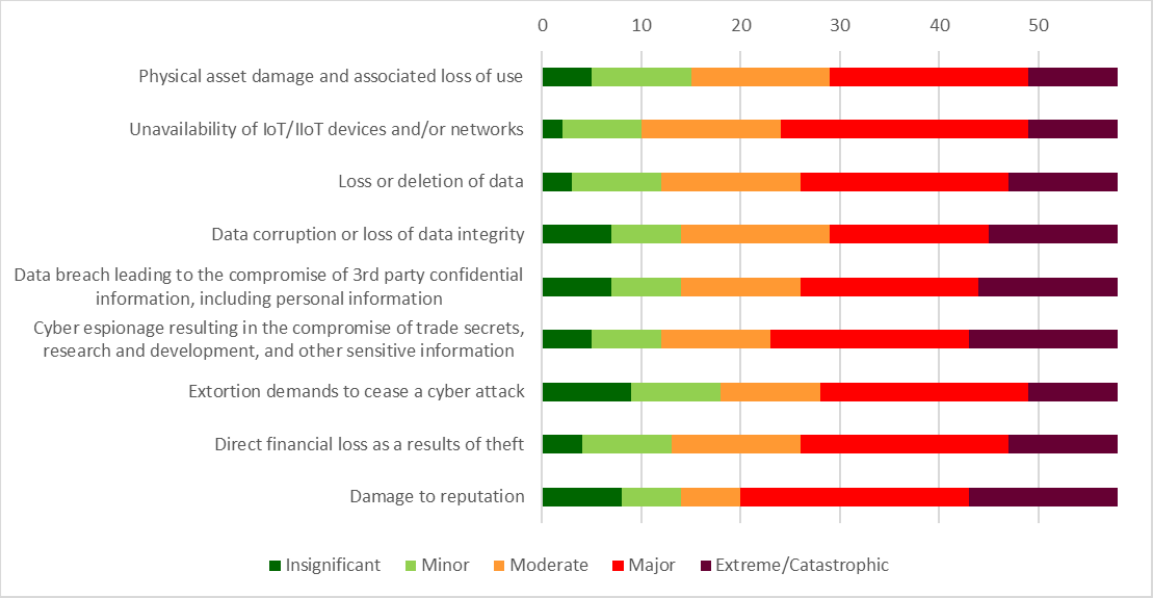


Figure 4-11: Risk (impact) related to IIoT

From the responses, the top three risks that have the most impact on IIoT in the transportation sector of SA are *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information*, with a mean of 3.6 (*Moderate*), combined second, *Loss or deletion of data*, *Damage to reputation* and *Unavailability of IIoT devices or networks* all with a mean of 3.5 (*Moderate*).

The 95% confidence intervals for the top three vulnerabilities related to IIoT systems are 0.3. This indicates that with 95% confidence, the population mean for each of the above is *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information* with a population mean of between 3.3 (mean – confidence = 3.6 – 0.3) to 3.9 (mean + confidence = 3.6 + 0.3), *Loss or deletion of data*, *Damage to reputation* and *Unavailability of IIoT devices or networks* all with a population mean of between 3.2 to 3.8 (*Moderate*).

The bottom three risks that are most likely to occur for IIoT in the transportation sector of South Africa: *Extortion demands to cease a cyberattack* with a mean of 3.2, *Physical asset damage and associated loss of use* with a mean of 3.3 and combined third, *Data corruption or loss of data integrity*,

Data breach leading to the compromise of 3rd party confidential information, including personal information and *Direct financial loss as a result of theft* all with a mean of 3.4 all *Moderate* impact.

Table 4-4: Frequency and descriptive statistics of risks (impact)

	Physical asset damage and associated loss of use	Unavailability of IIoT devices or networks	Loss or deletion of data	Data corruption or loss of data integrity	Data breach leading to the compromise of 3rd party confidential information, including personal information	Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information	Extortion demands to cease a cyberattack	Direct financial loss as a result of theft	Damage to reputation
Very low	5	2	3	7	7	5	9	4	8
Low	10	8	9	7	7	7	9	9	6
Medium	14	14	14	15	12	11	10	13	6
High	20	25	21	16	18	20	21	21	23
Very high	9	9	11	13	14	15	9	11	15
Mean	3.3	3.5	3.5	3.4	3.4	3.6	3.2	3.4	3.5
Median	3.5	4	4	3.5	4	4	4	4	4
Mode	4	4	4	4	4	4	4	4	4
Std Deviation	1.2	1.0	1.1	1.3	1.3	1.2	1.3	1.2	1.4
Variance	1.4	1.1	1.3	1.7	1.7	1.5	1.7	1.4	1.8
Kurtosis	-0.7	-0.2	-0.5	-0.8	-0.8	-0.5	-1.0	-0.6	-0.6
Skewness	-0.4	-0.5	-0.4	-0.4	-0.5	-0.6	-0.4	-0.5	-0.8
Confidence Level (95.0%)	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.4
Rank (Top)		2	2			1			2
Rank (Bottom)	2			3	3		1	3	

4.3.5 Risks of Unsecured IIoT (likelihood)

This relates to Question B4 of the questionnaire. Figure 4.12 shows the likelihood of the risks of unsecured IIoT devices in the transportation sector of South Africa. Table 4.5 shows the frequency and full descriptive statistics of the Risk Impact rating from *Very low* to *Very High*. To generate the descriptive statistics, the responses are rated from 1', *Very low*, to '5' *Very High.*

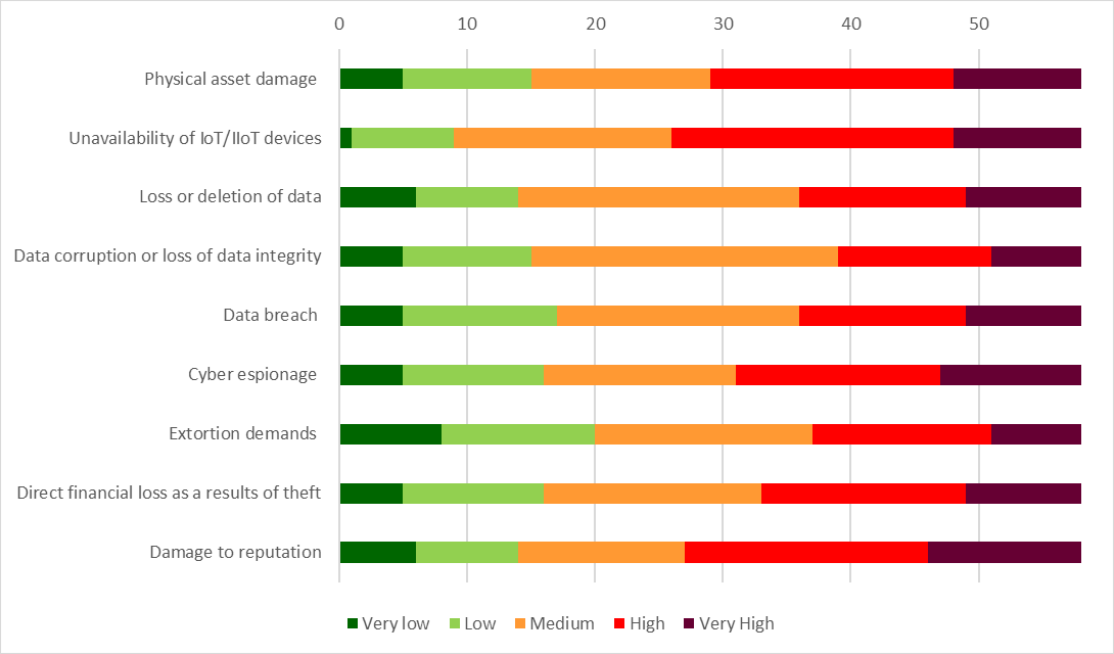


Figure 4-12: Risk (likelihood) related to IIoT

From the responses, the top three risks that are most likely to occur for IIoT in the transportation sector of SA are the *Unavailability of IIoT devices or networks* with a mean of 3.6 (*Medium*), *Damage to reputation* with a mean of 3.4 (also *Medium*), and combined third *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information* and *Physical asset damage and associated loss of use* with a mean of 3.3 (*Medium*).

The 95% confidence intervals for the top three vulnerabilities related to IIoT systems are 0.3. This indicates that with 95% confidence, the population mean for each of the above is *Unavailability of IIoT devices or networks* with a population mean of between 3.3 (mean – confidence = 3.6 – 0.3) to 3.9 (mean + confidence = 3.6 + 0.26), *Damage to reputation* with a population mean of 3.1 to 3.7 and *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information* and *Physical asset damage and associated loss of use* both with a population mean of between 3.0 to 3.6.

The bottom three risks that are most likely to occur for IIoT in the transportation sector of South Africa: *Extortion demands to cease a cyberattack* with a mean of 3.0, *Data corruption or loss of data integrity* with a mean of 3.1 and combined third, *loss or deletion of data*, *Data breach leading to the compromise of 3rd party confidential information, including personal information and Direct financial loss as a result of theft* all three with a mean of 3.2 all *Medium* likelihood.

Table 4-5: Frequency and descriptive statistics of risks (likelihood)

	Physical asset damage and associated loss of use	Unavailability of IIoT devices or networks	Loss or deletion of data	Data corruption or loss of data integrity	Data breach leading to the compromise of 3rd party confidential information, including personal information	Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information	Extortion demands to cease a cyberattack	Direct financial loss as a result of theft	Damage to reputation
Very low	5	1	6	5	5	5	8	5	6
Low	10	8	8	10	12	11	12	11	8
Medium	14	17	22	24	19	15	17	17	13
High	19	22	13	12	13	16	14	16	19
Very high	10	10	9	7	9	11	7	9	12
Mean	3.3	3.6	3.2	3.1	3.2	3.3	3.0	3.2	3.4
Median	3.5	4	3	3	3	3	3	3	4
Mode	4	4	3	3	3	4	3	3	4
Std Deviation	1.2	1.0	1.2	1.1	1.2	1.2	1.2	1.2	1.3
Variance	1.5	1.0	1.4	1.2	1.4	1.5	1.5	1.4	1.6
Kurtosis	-0.8	-0.5	-0.6	-0.4	-0.8	-0.9	-0.9	-0.8	-0.7
Skewness	-0.4	-0.3	-0.2	0.0	0.0	-0.2	-0.1	-0.2	-0.5
Confidence Level (95.0%)	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3
Rank (Top)	3	1				3			2
Rank (Bottom)			3	2	3		1	3	

4.3.6 Risks of Unsecured IIoT (Impact and Likelihood)

As discussed in Section 2.2.2, risk is defined as *Impact* times *Probability/Likelihood*. The mean from the likelihood of each risk from Section 4.3.5 is taken, as well as the mean from the impact of the threat from Section 4.3.4. The means of each threat's likelihood vs the mean of each threat's impact is plotted in Figure 4.13 and displayed in Table 4.6. The risk for each category is listed in Table 4.6 and illustrated in Figure 4.13 considering both the mean impact and likelihood ratings. Table 4.6 calculates the risk as the product of the mean for impact and likelihood and ranges from 1 to 25. The highest risk is in the top right corner, and the lowest is in the bottom left corner.

Table 4-6: Calculated Risk for IIoT

Risk Description	Impact	Likelihood	Risk
Unavailability of IIoT devices or networks	3.5	3.6	12.6
Damage to reputation	3.5	3.4	12.0
Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information	3.6	3.3	11.8
Direct financial loss as result of theft	3.4	3.2	11.1
Loss or deletion of data	3.5	3.2	11.1
Physical asset damage and associated loss of use	3.3	3.3	11.0
Data breach leading to the compromise of 3rd party confidential information, including personal information	3.4	3.2	10.8
Data corruption or loss of data integrity	3.4	3.1	10.4
Extortion demands to cease a cyberattack	3.2	3.0	9.6

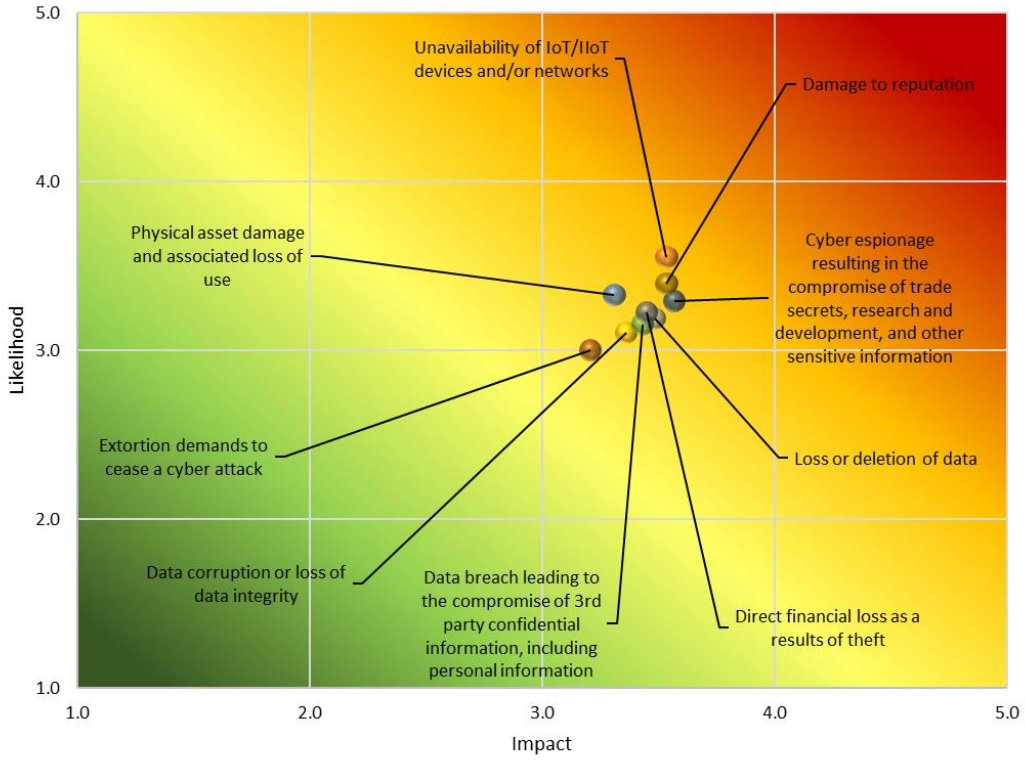


Figure 4-13: Risk (Impact vs Likelihood)

According to Figure 4.13, the level of risk is determined by multiplying the probability by the impact. A higher number indicates a greater risk. Risks depicted in Figure 4.13 are more significant when located in the upper right-hand corner (red) and less significant when located in the lower left-hand corner (green). From Figure 4.13, it is observed that the top three risks for IIoT in the transportation sector of SA are the *Unavailability of IIoT devices or networks*, secondly, *Damage to reputation* and *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information*. Comparing this to the top three threats (new or existing) likely to be introduced by IIoT in the transport sector of SA, *cyber espionage* and the top threat, *cyber espionage,* align with the risk of *cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information* showing great consistency.

We can also see from Figure 4.14 that almost all the risks are clustered together apart from the bottom three risks. The bottom three risks for IIoT in the transportation sector of SA are *Extortion demands to cease a cyberattack*, *Data corruption or loss of data integrity* and *Physical asset damage and associated loss of use*.

Section 6.2.3 discusses the results further, including a unique analysis of the implications for the transport sector.

4.3.7 Occurrence of Threats related to an IIoT Environment in the Transport Sector in South Africa

This relates to Question B5 of the questionnaire. Figure 4.14 shows the responses from the questionnaire. The respondents are asked to indicate if any of the threats occurred in their organisation or an IIoT environment that they have encountered in the transport sector of South Africa. 29% of respondents indicated that a threat did occur, and 28% of respondents did not have a threat occur in their IIoT environment. 24% is *Not sure*, 12% indicated *Maybe*, while 7% *Can't disclose.* From this, it could be concluded that only 28% did not have a threat occur in their IIoT environment. In comparison, the remaining 72% might have had a threat in their IIoT environment. This strengthens the need to secure IIoT systems, as 72% of respondents might have a threat occur in their IIoT environment.

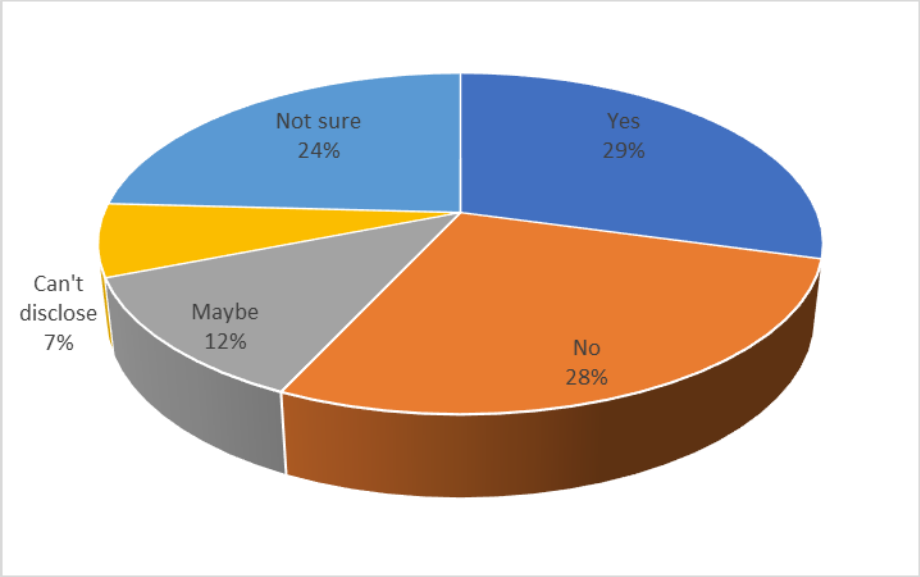


Figure 4-14: Occurrence of threats

4.3.8 Type of IIoT or ICS/SCADA Devices in an IIoT Environment in the Transport Sector in South Africa

This relates to Question B6 of the questionnaire. Figure 4.15 shows that 75% of the respondents have boardroom/video conferencing equipment, 68% have CCTV / Smart cameras, 55% have vehicle tracking/monitoring, 51% also have sensors (general), 46% have IIoT devices for cargo tracking as well as environmental monitoring devices (e.g. weather, wind, fire detection), 45% have industrial Wi-Fi / LTE, 45% have building management systems (e.g. aircon controllers), 43% have equipment monitoring, 43% have cargo monitoring (e.g. reefer monitoring, status of cargo), 40% have equipment tracking, 38% have smart metering (e.g. energy monitoring), 9% have smart parking and 9% have IIoT devices for traffic flow management.

Section 6.2.2 discusses the results further, including a unique analysis of the implications for the transport sector.

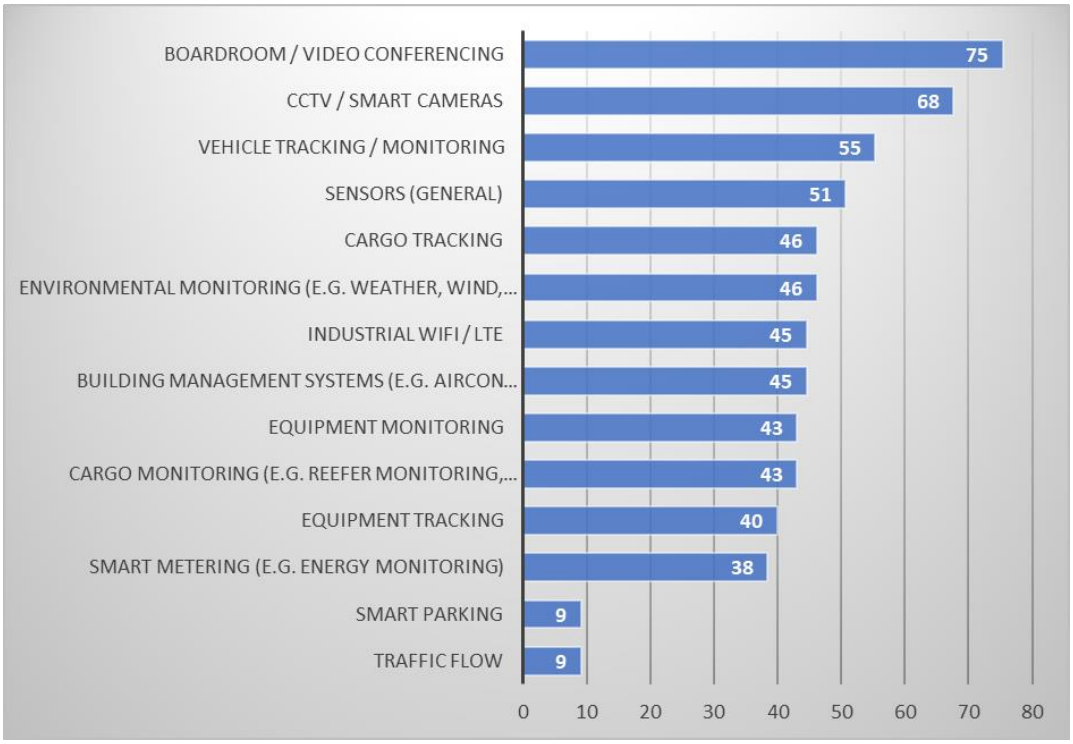


Figure 4-15: Type of IIoT devices

4.4 Organisational Factors Influencing IIoT

This section relates to the research objective to determine the Organisational factors influencing IIoT security in the transport sector of South Africa.

4.4.1 Size and Structure

This relates to Question C1 of the questionnaire. Figure 4.16 indicates how respondents see the size and structure of the support for their IIoT environment in the transport sector of SA. Table 4.7 shows the frequency and full descriptive statistics of the support for IIoT ranging from *No staff* to *Dedicated department dealing with it*. To generate the descriptive statistics, the responses are rated from '1', *No staff*, '2' *Ad hoc staff*, '3' *Allocated as part of a project*, '4' *Part of daily task* and '5' *Dedicated department dealing with it.*

Table 4-7: Frequency and descriptive statistics of support for IIoT environment

	Employees supporting IIoT	Security staff	IIoT security staff
1 – No staff	4	7	12
2 – Ad hoc staff	17	17	14
3 – Allocated as part of a project	21	12	10
4 – Part of daily tasks	7	14	18
5 – Dedicated department dealing with it	9	8	4

	Employees supporting IIoT	Security staff	IIoT security staff
Mean	3	2.98	2.79
Median	3	3.00	3.00
Mode	3	2.00	4.00
Standard Deviation	1.15	1.26	1.28
Sample Variance	1.33	1.60	1.64
Kurtosis	-0.62	-1.09	-1.26
Skewness	0.35	0.09	-0.01
Confidence Level (95.0%)	0.30	0.33	0.34

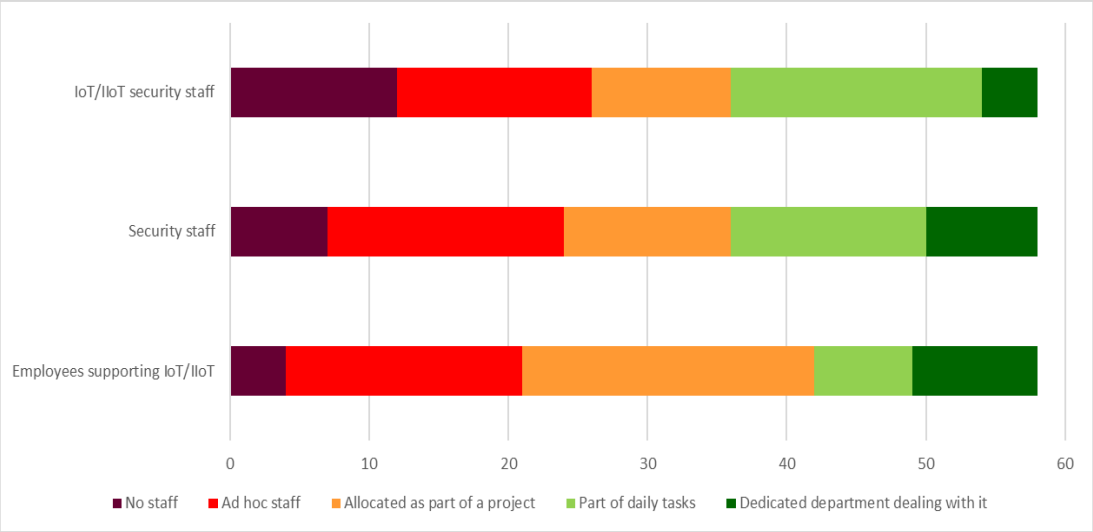


Figure 4-16: Size and structure of support for IIoT environment

From the responses, the *Employees supporting IIoT* have a mean of 3 (*Allocated as part of a project*), *Security staff* with a mean of 2.98 (leaning towards *Allocated as part of a project*), and *IIoT security staff* with a mean of 2.79 (also leaning towards *Allocated as part of a project*).

The 95% confidence intervals for the staff supporting IIoT systems are 0.3 for *Employees supporting IIoT*, 0.33 for *Security staff* and 0.34 for *IIoT security staff*. This indicates that with 95% confidence, the population mean for each of the above are *Employees supporting IIoT* with a population mean of between 2.7 (mean – confidence = 3.0 – 0.3) to 3.3 (mean + confidence = 3.0 + 0.3), *Security staff* with a population mean of 2.65 to 3.31 and *IIoT security staff* with a population mean of between 2.45 to 3.13.

Section 6.3.1 discusses the results further, including a unique analysis of the implications for the transport sector.

4.4.2 Security Strategy

This relates to Question C2 of the questionnaire. Figure 4.17 and Table 4.8 indicates how respondents see the maturity of the security strategy for their IIoT environment in the transport sector of SA. To generate the descriptive statistics, the responses are rated from '1', *Initial* to '5' *Focus on process improvement.*

Table 4-8: Frequency and descriptive statistics of security strategy

	Cybersecurity roadmap / strategy supporting IIoT	Risk assessment for IIoT	Governance processes for IIoT	Innovative culture in the organisation	Security culture in the organisation	Senior / Executive understanding of IIoT security risks
Initial	20	15	14	23	16	21
Managed	20	23	23	16	15	20
Defined	13	12	11	10	15	7
Quantitatively Managed	3	5	9	7	9	7
Focus on process improvement	2	3	1	2	3	3
Mean	2.09	2.28	2.31	2.12	2.45	2.16
Median	2	2	2	2	2	2
Mode	2	2	2	1	1	1
Std Deviation	1.05	1.10	1.06	1.17	1.20	1.20
Variance	1.10	1.22	1.13	1.37	1.44	1.43
Kurtosis	0.42	0.14	-0.57	-0.40	-0.81	-0.14
Skewness	0.87	0.80	0.52	0.78	0.38	0.90
Confidence Level (95.0%)	0.28	0.29	0.28	0.31	0.32	0.31
Rank (Top)		3	2		1	
Rank (Bottom)	1			2		3

Figure 4-17: Maturity of Security strategy of IIoT environment

From the responses, the mean for responses of the maturity of *Cybersecurity roadmap/strategy supporting IIoT* for IIoT environment is 2.09, the mean for the maturity of *the Risk assessment for IIoT* is 2.28, the mean for *Governance processes for IIoT* is 2.31, *Innovative culture in the organisation* maturity have a mean of 2.12, *Security culture in the organisation* a mean of 2.45 and *Senior / Executive understanding of IIoT security risks* a mean of 2.16.

The 95% confidence interval for the maturity of the *Cybersecurity roadmap/strategy supporting IIoT* environment is 0.28, *Risk assessment for IIoT* is 0.29, *Governance processes for IIoT* is 0.28, *Innovative culture in the organisation* is 0.31, *Security culture in the organisation* is 0.32 and *Senior / Executive understanding of IIoT security risks* one of 0.31. This indicates that with 95% confidence, the population mean for each of the above is *Cybersecurity roadmap/strategy supporting IIoT* with a population mean of between 1.81 (mean – confidence = 2.09 – 0.28) to 2.36 (mean + confidence = 2.09 + 0.28), *Risk assessment for IIoT* with a population mean of 1.99 to 2.57, *Governance processes for IIoT* with a population mean of 2.03 to 2.59, *Innovative culture in the organisation* with a population mean of 1.81 to 2.43, *Security culture in the organisation* with a population mean of 2.13 to 2.76 and *Senior / Executive understanding of IIoT security risks* with a population mean of 1.84 to 2.47.

The CMM, as discussed in Section 2.2.3.2, for each of these are displayed in Figure 4.18 to Figure 4.23. The current state depicts the results from the questionnaire and the desired state as discussed in Section 2.2.3.2.

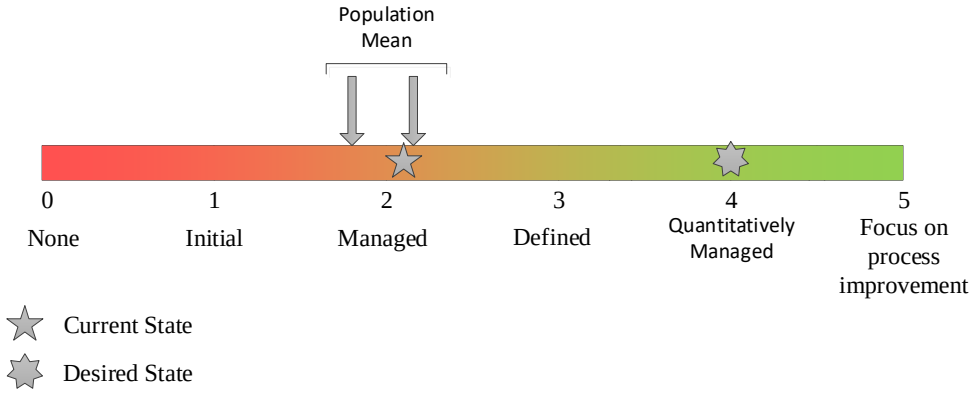


Figure 4-18: Maturity of cybersecurity roadmap / strategy

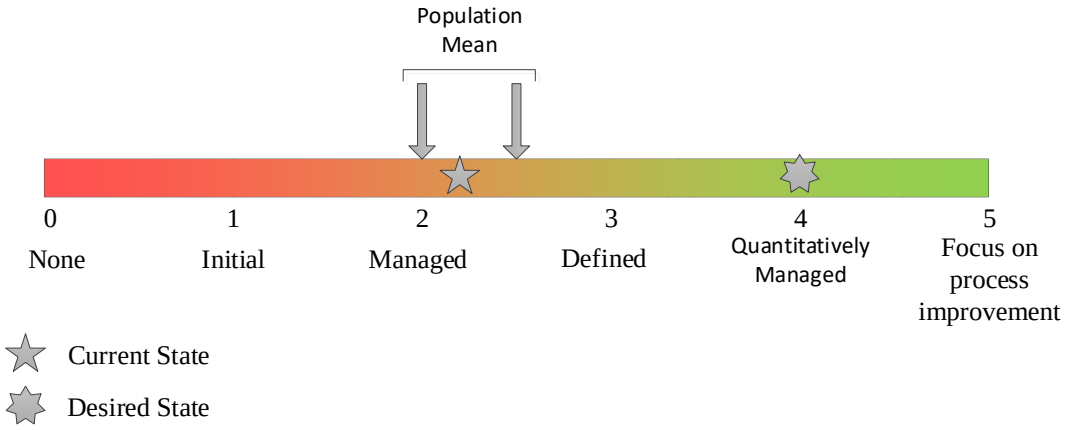


Figure 4-19: Maturity of risk assessment / appetite

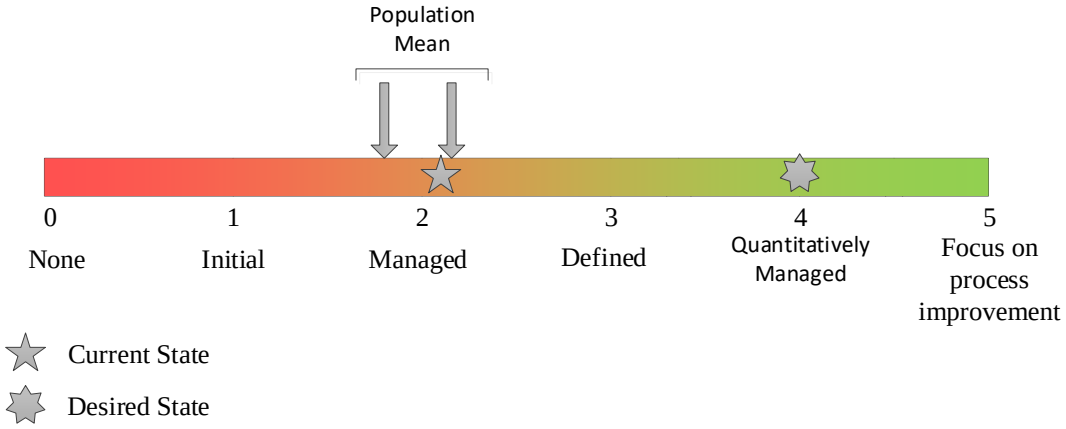


Figure 4-20: Maturity of governance processes for IIoT

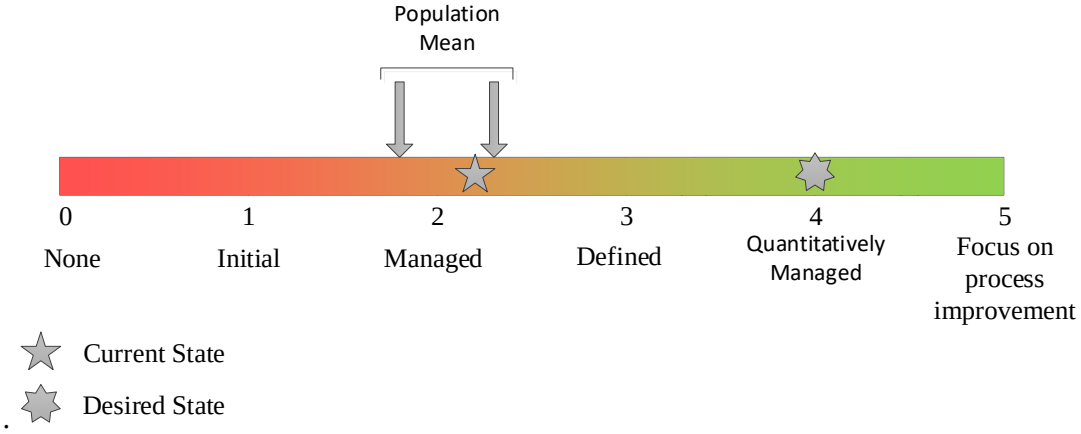


Figure 4-21: Maturity of innovative culture

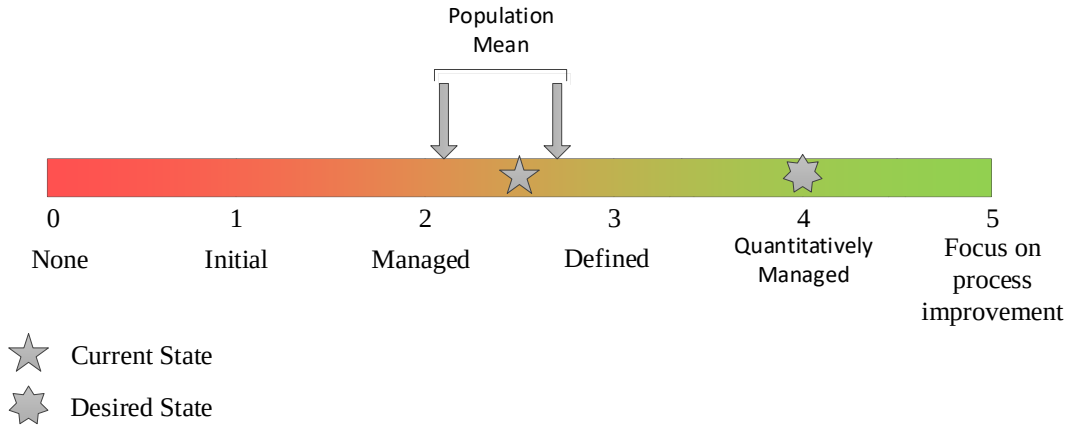


Figure 4-22: Maturity of security culture

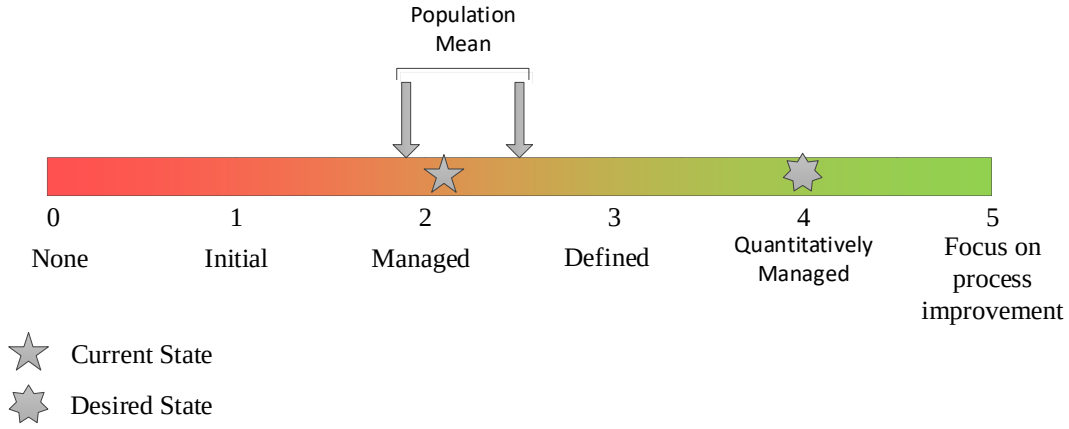


Figure 4-23: Senior / Executive understanding of IIoT security risks

Sections 6.3.2 – 6.3.6 discusses the results further, including a unique analysis of the implications for the transport sector.

4.4.3 Responsible for the Security of IIoT

This relates to Question C3 of the questionnaire. Figure 4.24 indicates who respondents believe is responsible for the security of IIoT in their organisation or an organisation they have encountered in the transport sector of SA. Almost half of the respondents indicated that *All employees* are responsible for the security of IIoT 43%; 22% of respondents indicated that security is responsible, 16% indicated IT, 10% indicated *Engineering/OT* are responsible, 7% indicated that both *The Board* are responsible and only a few indicated that *A combination of groups, from Executive Management down to the users designing, implementing, and interacting with the systems and IIoT devices* are responsible with 2%.

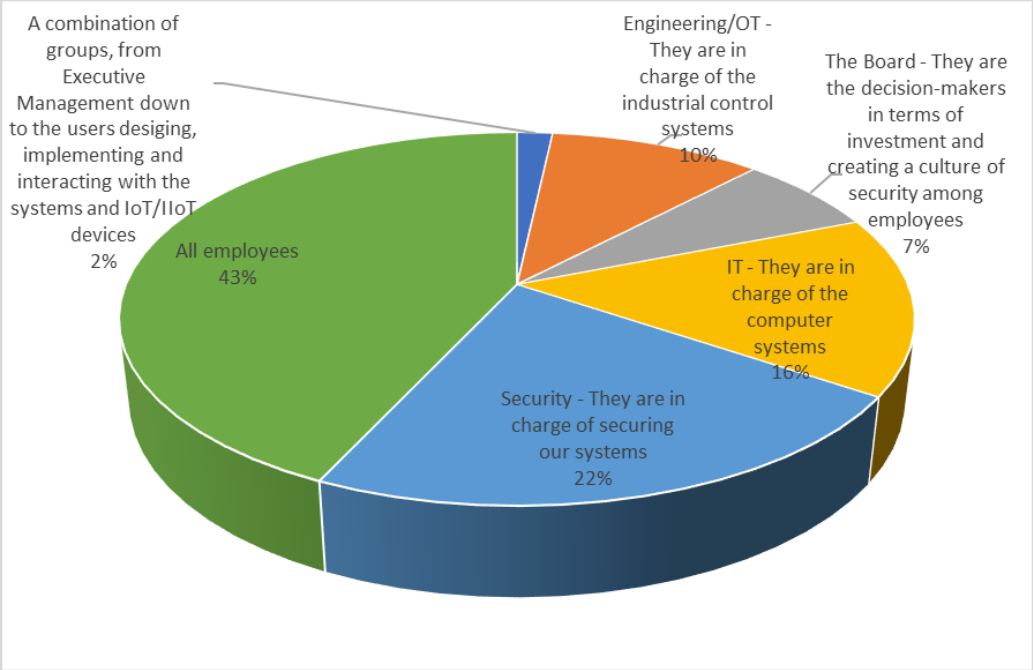


Figure 4-24: Responsible for the security of IIoT

4.4.4 Maturity of Security for IIoT

This relates to Question C4 of the questionnaire. Figure 4.25 indicates how respondents see the security maturity of their IIoT environment. 33% of respondents indicated that the maturity of their IIoT environment is *Basic*, 29% indicated that the maturity of their environment is *Established*, and 29% also indicated that their environment is *Evolving*. Only 7% of IIoT environments are *Advanced*, and none are *Leading*. To generate the descriptive statistics, the responses are rated from '1', *Basic* to '5' *Leading*.

Table 4.9 contains descriptive statistics.

Table 4-9: Frequency and descriptive statistics for Maturity of security of IIoT environment

	Frequency
0 - None	1
1 - Basic (Very minimal or basic level of controls)	19
2 - Evolving (Inconsistently applied controls)	17
3 - Established (Controls in place, but there is a need for enhancement)	17
4 - Advanced (Control are consistently applied)	4
5 - Leading (Controls are established, consistently applied, regularly reviewed, and coordinated)	0
Mean	2.07
Median	2
Mode	1
Standard Deviation	0.99
Sample Variance	0.98
Kurtosis	-0.89
Skewness	0.20
Confidence Level (95.0%)	0.26

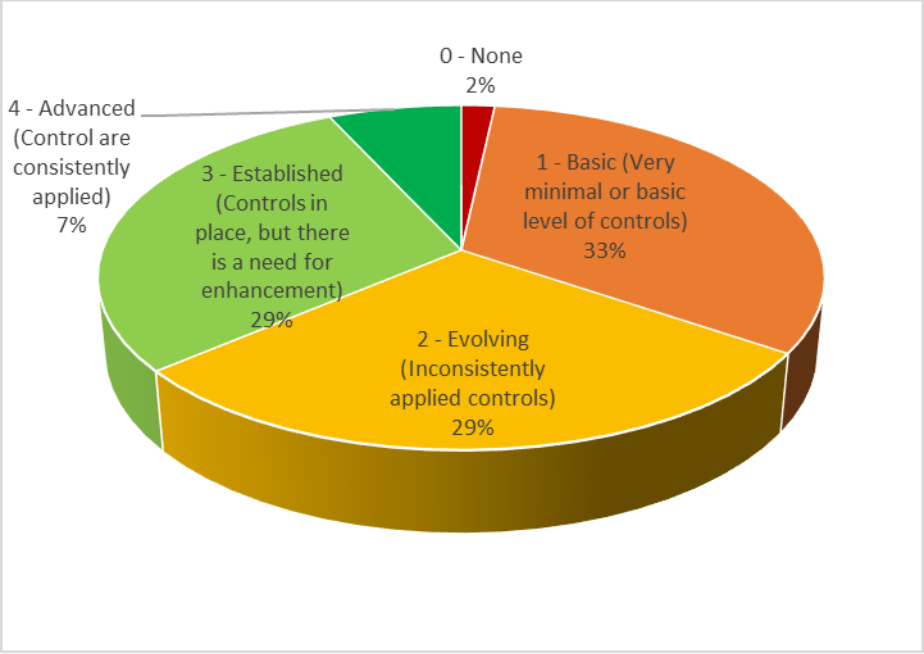


Figure 4-25: Maturity of security of IIoT environment

From the responses, the mean for responses of the maturity of cybersecurity for IIoT environment is 2.07, which relates to the maturity of *Evolving (Inconsistently applied controls).*

The 95% confidence interval for this is 0.26. This indicates that with 95% confidence, the population mean for the maturity of security for the IIoT environment in the transport sector of SA is between 1.81 (mean – confidence = 2.07 – 0.26) to 2.33 (mean + confidence = 2.07 + 0.26). This indicates that the population mean for the maturity of cybersecurity for IIoT environments, as per the CMM discussed in Section 2.2.4.3, is *Evolving (Inconsistently applied controls)*. The CMM is displayed in Figure 4.26.

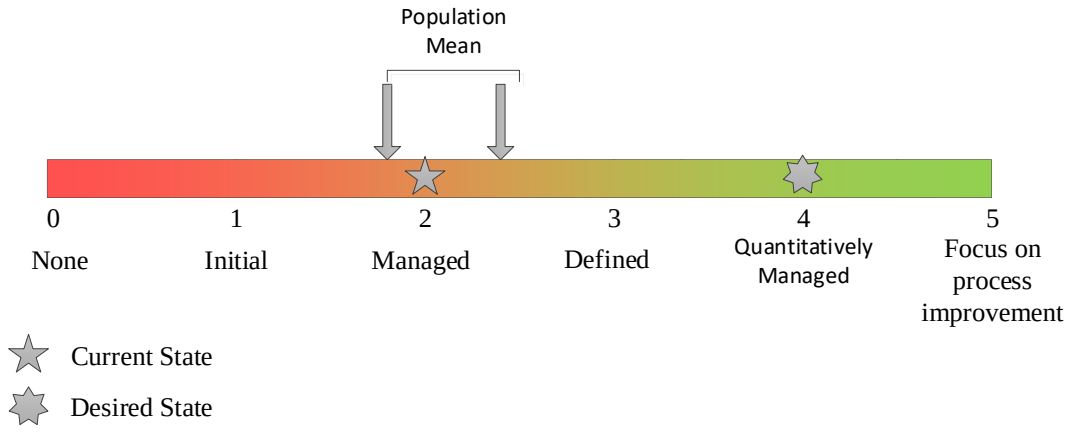


Figure 4-26: IIoT cybersecurity maturity

4.5 Procedural Factors Influencing IIoT

This section relates to the research objective to determine the Procedural factors influencing IIoT security in the transport sector of South Africa.

4.5.1 Maturity of Incident Response for IIoT Systems

This relates to Question D1 of the questionnaire. Figure 4.27 indicates how respondents see the maturity of incident response for their IIoT environment. To generate the descriptive statistics, the responses are rated from '0', *None / Not implemented*, '1', *Initial* to '5' *Optimised*. The results are displayed in Table 4.10.

From the responses, the mean for responses of the maturity of the *organisation has an incident response plan* for IIoT environment is 2.4, which is between managed (Process characterised for projects and is often reactive) and defined (Processes characterised for the organisation and is proactive) and the mean for the maturity of *Incident response plan address IIoT risk* is 1.9 which is strongly leaning towards managed (Process characterised for projects and is often reactive).

Table 4-10: Frequency and descriptive statistics for Maturity of security of IIoT environment

	Organisation has an incident response plan	Incident response plan address IIoT risk
None / Not implemented (0)	4	7
Initial (1)	14	20
Managed (2)	13	15
Defined (3)	15	8
Quantitatively Managed (4)	6	4
Optimised (5)	6	4
Mean	2.40	1.90
Median	2	2
Mode	3	1
Standard Deviation	1.41	1.37
Sample Variance	2.00	1.88
Kurtosis	-0.71	-0.06
Skewness	0.26	0.74
Confidence Level (95.0%)	0.37	0.36

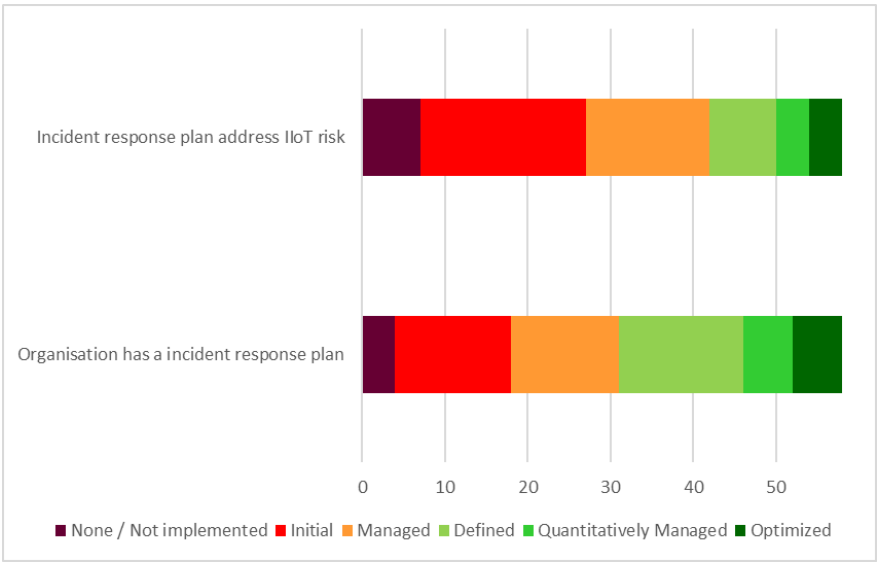


Figure 4-27: Maturity of security of IIoT environment

The 95% confidence intervals for the maturity of the *organisation have an incident response plan* for IIoT environment is 0.37, and the maturity of an *Incident response plan addressing IoT risk* is 0.36. This indicates that with 95% confidence, the population mean for the maturity of the *organisation has an incident response plan* for IIoT environment is between 2.02 (mean – confidence = 2.4 – 0.37) to 2.77 (mean + confidence = 2.4 – 0.37) and *Incident response plan address IoT risk* with a population mean of 1.54 to 2.26.

The CMM is displayed in Figure 4.28 and Figure 4.29. Section 6.4.1 discusses the results further, including a unique analysis of the implications for the transport sector.

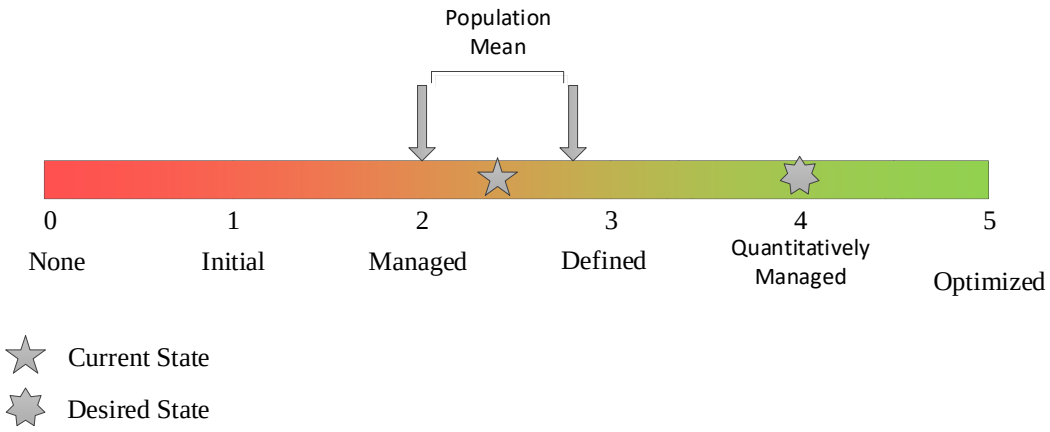


Figure 4-28: Organisation has an incident response plan

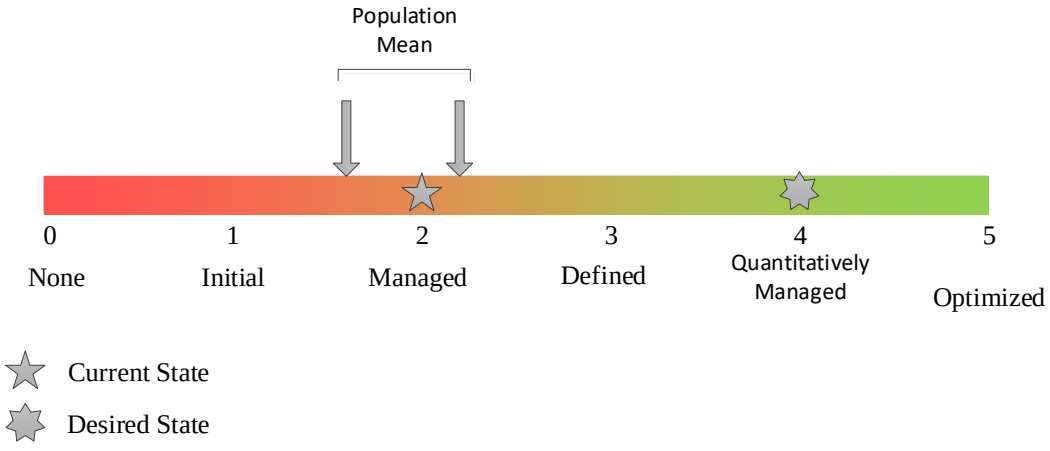


Figure 4-29: Incident response plan address IIoT risk

4.5.2 Maturity of IIoT Policies, Procedures, Frameworks, and Standards for IIoT Systems

This relates to Question D2 of the questionnaire. Figure 4.30 indicates how respondents see the maturity of IIoT policies, procedures, frameworks, and standards for their IIoT environment in the transport sector of South Africa. To generate the descriptive statistics, the responses are rated from '0', *None / Not implemented*, '1', *Initial* to '5' *Optimised*. The results are displayed in Table 4.11

Table 4-11: Frequency and descriptive statistics for Maturity of IIoT policies, procedures, frameworks, and standards

	General security policies/procedures implemented	IIoT security policies/procedures/ controls implemented	Governance processes for IIoT	Control framework for IIoT
None / Not implemented	4	6	7	7
Initial	15	23	22	23
Managed	9	12	10	10
Defined	21	11	13	12
Quantitatively Managed	8	4	6	6
Optimised	1	2	0	0
Mean	2.29	1.83	1.81	1.78
Median	3	1.5	1.5	1
Mode	3	1	1	1
Standard Deviation	1.24	1.26	1.22	1.21
Sample Variance	1.54	1.58	1.49	1.48
Kurtosis	-0.88	-0.13	-0.98	-0.91
Skewness	-0.13	0.67	0.32	0.39
Confidence Level (95.0%)	0.33	0.33	0.32	0.32

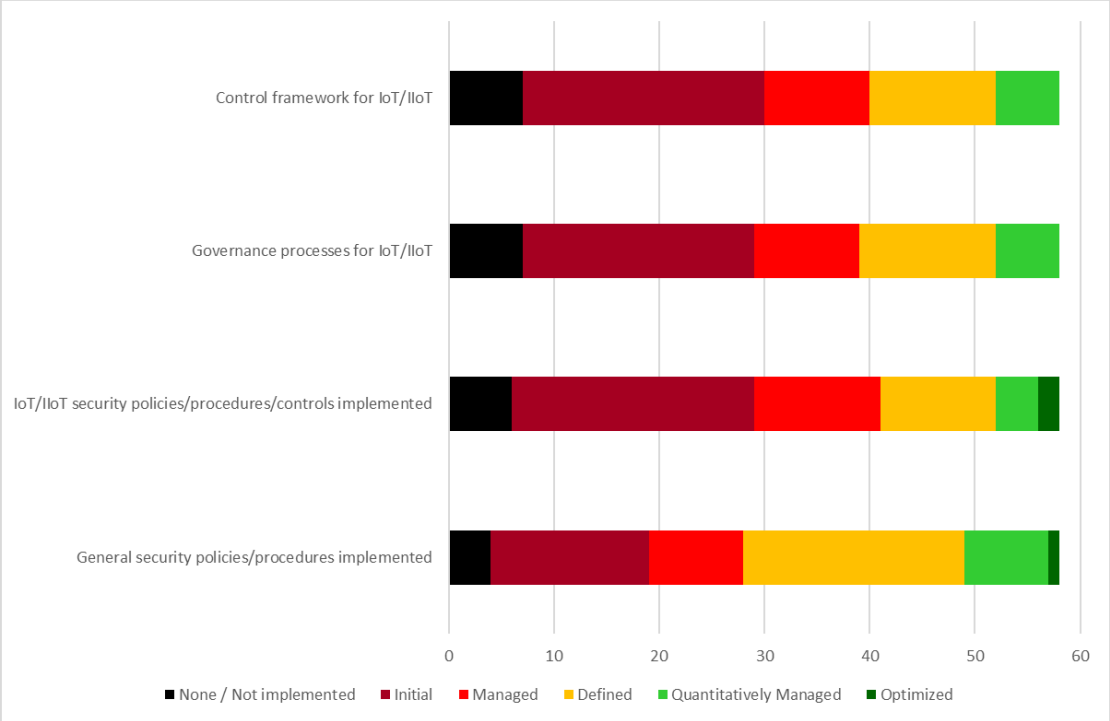


Figure 4-30: Maturity of IIoT policies, procedures, frameworks, and standards

From the responses, the mean for responses of the maturity of *General security policies/procedures implemented* for IIoT environment is 2.29, which is between managed (Processes characterised for projects and is often reactive) and defined (Processes characterised for the organisation and is proactive), the mean for the maturity of *IIoT security policies/procedures/controls implemented* is 1.83, the mean for the maturity of *Governance processes for IIoT* is 1.81 and the mean for the maturity of *Control framework for IIoT* is 1.78 all strongly leaning towards managed (Process characterised for projects and is often reactive).

The 95% confidence interval for the above is 0.33 for *General security policies/procedures implemented* for IIoT environment, 0.33 for the maturity of *IIoT security policies/procedures/controls implemented*, 0.32 for *Governance processes for IIoT*, and 0.32 for *Control framework for IIoT*. This indicates that with 95% confidence, the population mean for the maturity of the *General security policies/procedures implemented* for IIoT environment is between 1.97 (mean – confidence = 2.29 – 0.33) to 2.62 (mean + confidence = 2.29 + 0.33), *IIoT security policies/procedures/controls implemented* with a population mean of 1.50 to 2.16, *Governance processes for IIoT* with a population mean of between 1.49 to 2.13 and *Control framework for IIoT* with a population mean of 1.46 to 2.10.

The CMM is displayed in Figure 4.31 to Figure 4.34. Section 6.4.3 discusses the results further, including a unique analysis of the implications for the transport sector.

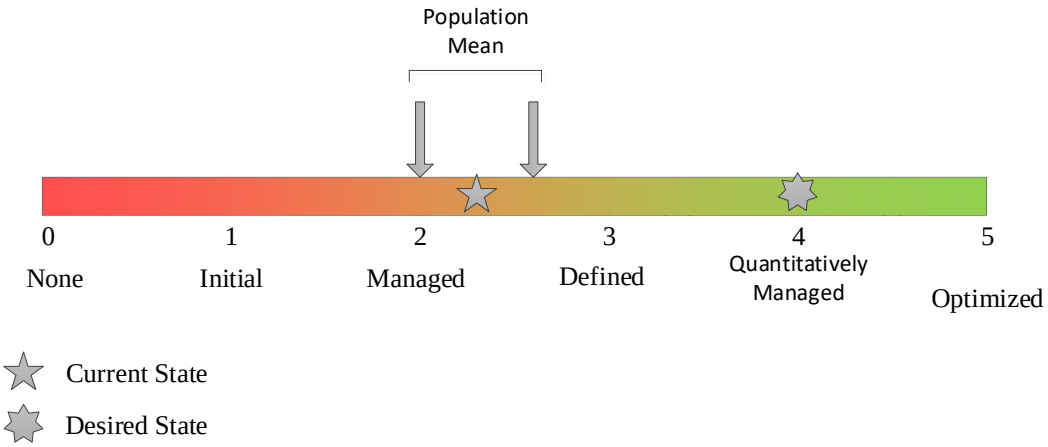


Figure 4-31: General security policies/procedures implemented

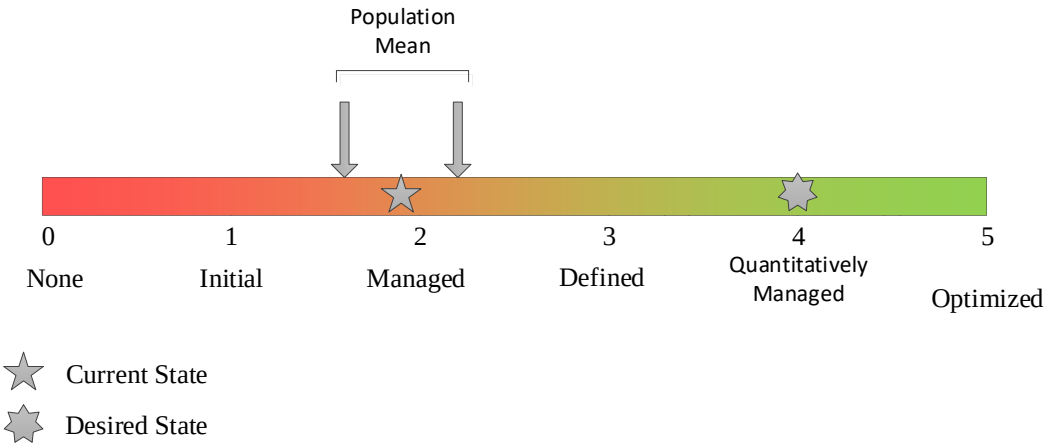


Figure 4-32: IIoT security policies/procedures/controls implemented

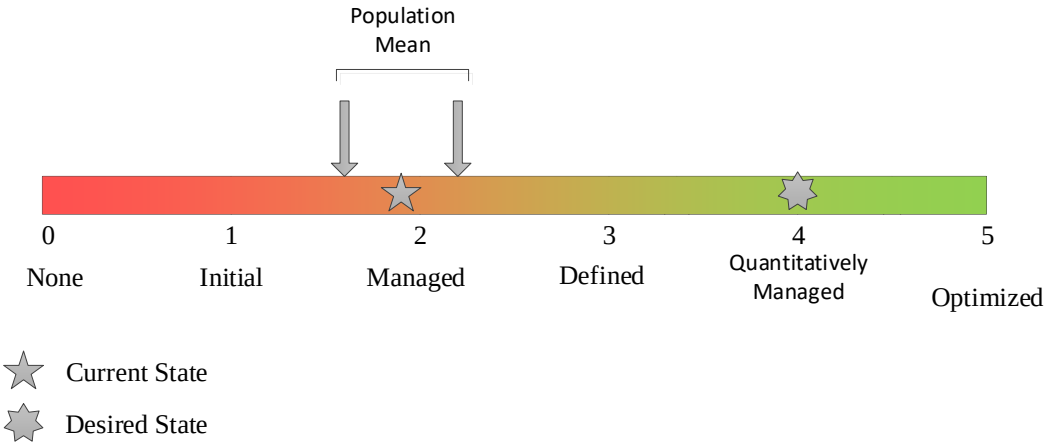


Figure 4-33: Governance processes for IIoT

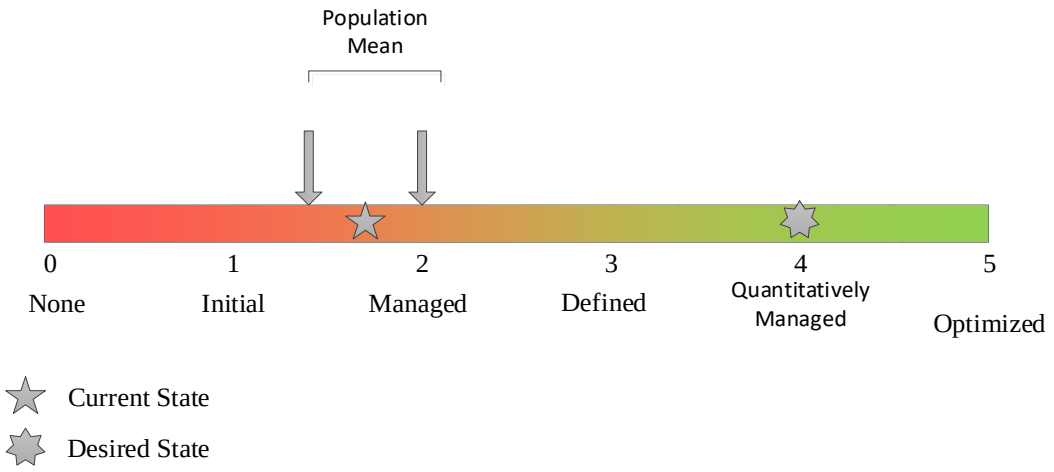


Figure 4-34: Control framework for IIoT

4.5.3 Control Frameworks Implemented or Adopted for IIoT

This relates to Question D3 of the questionnaire. Figure 4-35 indicates the control frameworks used by the participants to secure their IIoT environment in the transport sector of SA.

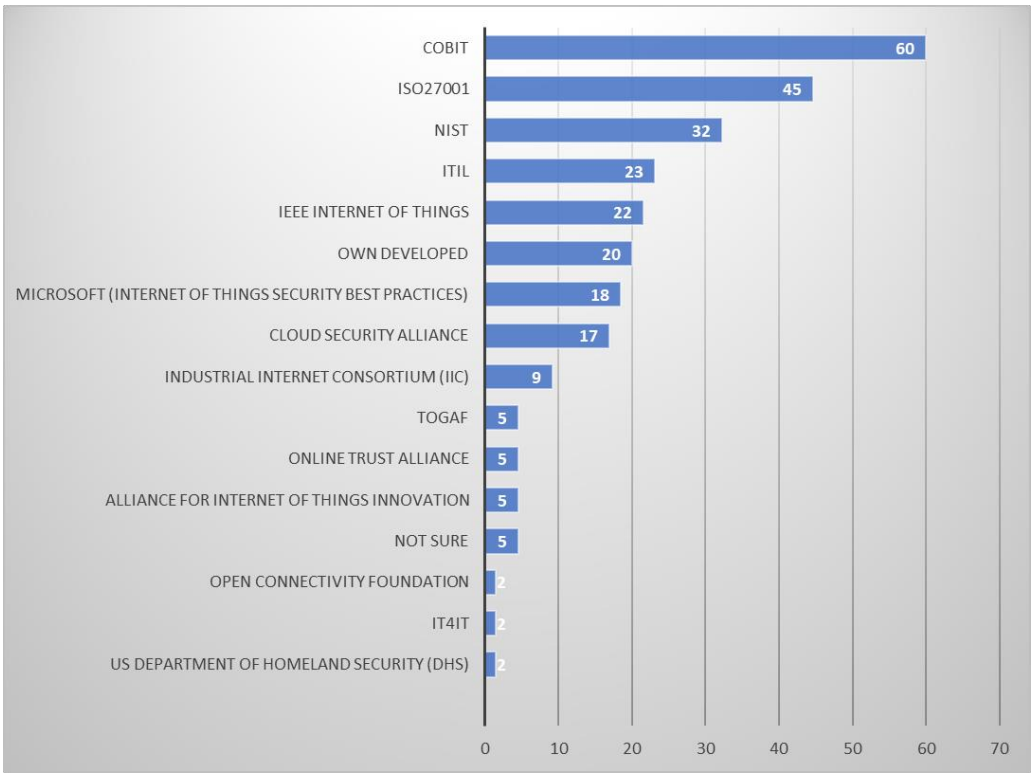


Figure 4-35: Control frameworks implemented or adopted

The responses note that the top three frameworks used by the respondents to govern and secure their IIoT environments are COBIT, ISO 27001 series and NIST. COBIT is used by around 60% of the respondents, more than ISO 27001 at 45% and NIST at 32%. COBIT is suitable from a governance

and security perspective; however, ISO 27001 and NIST are more suitable as they focus more on security. The bottom three responses from the users are around 2% of the respondents, for all three namely, *US Department of Homeland Security*, *IT4IT* and *Open Connectivity Foundation*. Around 5% of respondents were not sure what control frameworks are implemented or adopted.

4.5.4 Threat Intelligence

This relates to Question D4 of the questionnaire. Figure 4.36 indicates that 26% of respondents *Rely on staff to know when to search out events*, 25% of respondents rely on *Review of audit logs* to detect threats, 26% *Use anomaly detection tools (SIEM/SIC) to identify trends*, 17% *Third-party intelligence provided*, 4% had *None* and 2% *Other* sources to detect threats for IIoT in the transport sector of South Africa. Other sources include Cisco Umbrella - DNS Layer Security at a Global Scale and OSSIM.

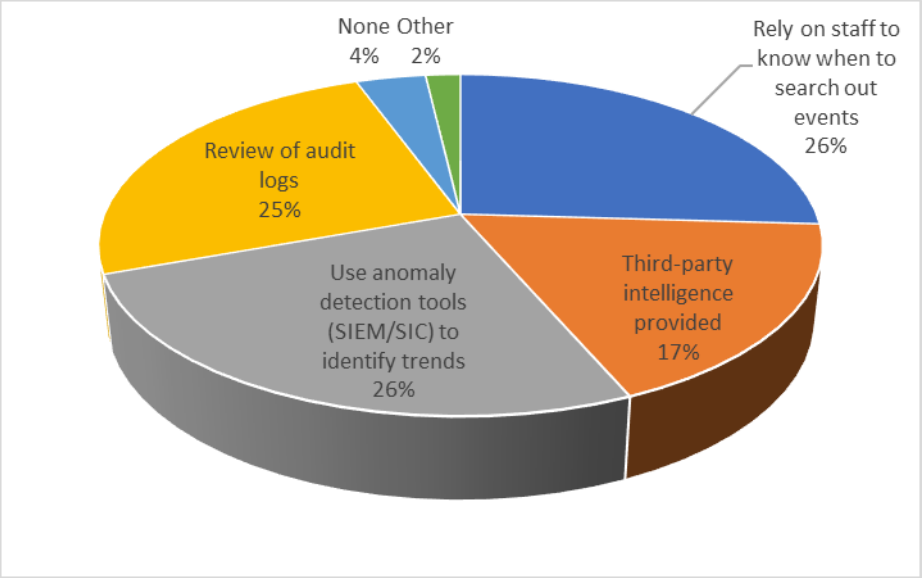


Figure 4-36: Type of intelligence used

4.5.5 Confidence of Controls to Mitigate the Threats and Risks

This relates to Question D5 of the questionnaire. The respondents are asked how confident they are that the controls mitigate the IIoT threats and risks in the transport sector of South Africa. 36% indicated that they are *somehow confident*, 29% are *Not confident at all*, 23% are *Moderately confident*, 10% are *Confident*, and only 2% are *Very confident*. This indicates that more than 50% are not confident in the controls to mitigate the threats and risks. Figure 4.37 contains the results.

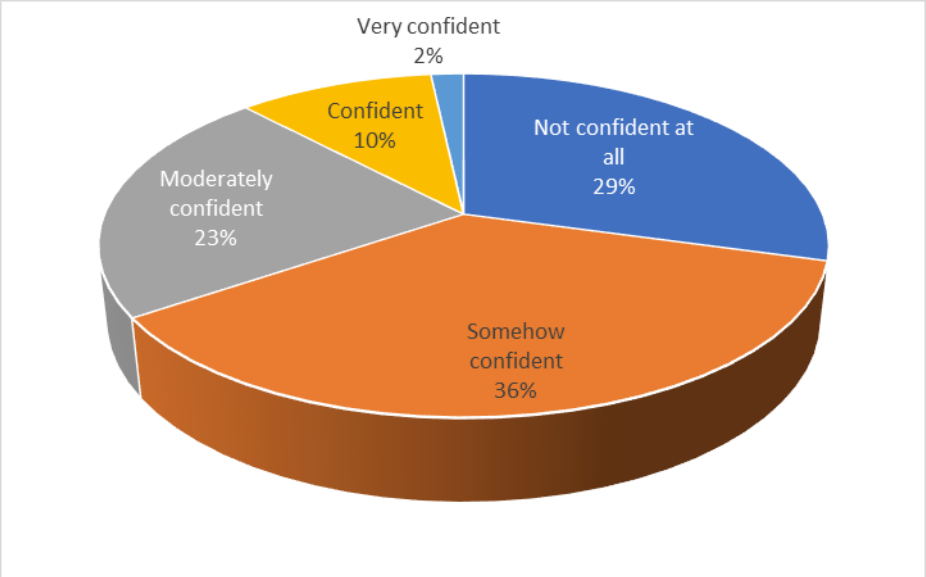


Figure 4-37: Confidence of controls mitigating IIoT threats and risks

4.5.6 What are the Top Three Priorities when Implementing Effective Controls?

This relates to Question D6 of the questionnaire. Figure 4.38 indicates that the top three priorities when it comes to implementing effective controls for the security of IIoT environment in the transport sector in SA are *Protecting health and safety of employees* selected by 26 or 45% of the respondents, *Meeting regulatory compliance* selected by 20 or 34% of the respondents and *Protecting company reputation and brand* selected by 19 or 33% respondents.

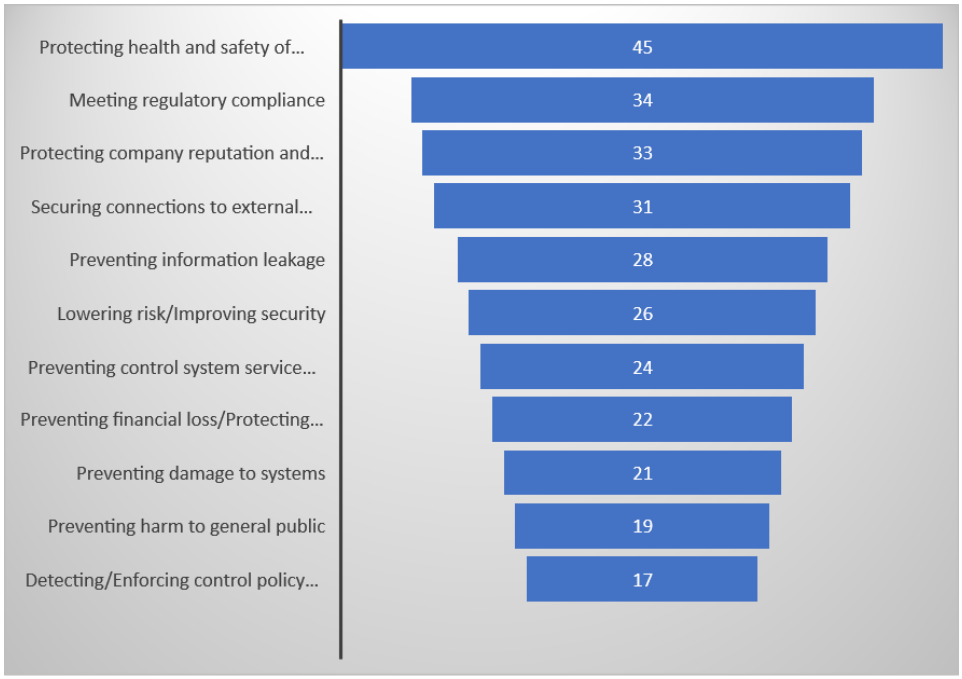


Figure 4-38: Top three priorities when it comes to implementing effective controls (%)

The bottom three or three least priorities when it comes to implementing effective controls for the security of IIoT environment in the transport sector in SA *Detecting/Enforcing control policy violations* selected by 10 or 17% of the respondents, *Preventing harm to general public* selected by 11 or 19% respondents and *Preventing damage to systems* selected by 12 or 21% of respondents.

4.5.7 Maturity of Controls to Protect Against the Risks Imposed by new IIoT

This relates to Question D7 of the questionnaire. The respondents are asked to rate the maturity of controls to protect against the risks imposed by new IIoT in their organisation or an IIoT environment that they have encountered in the transport sector in South Africa. Figure 4.39 indicates that. To generate the descriptive statistics, the responses are rated from '0', *None / Not implemented*, '1', *Initial* to '5' *Optimised*. The results are displayed in Table 4.12.

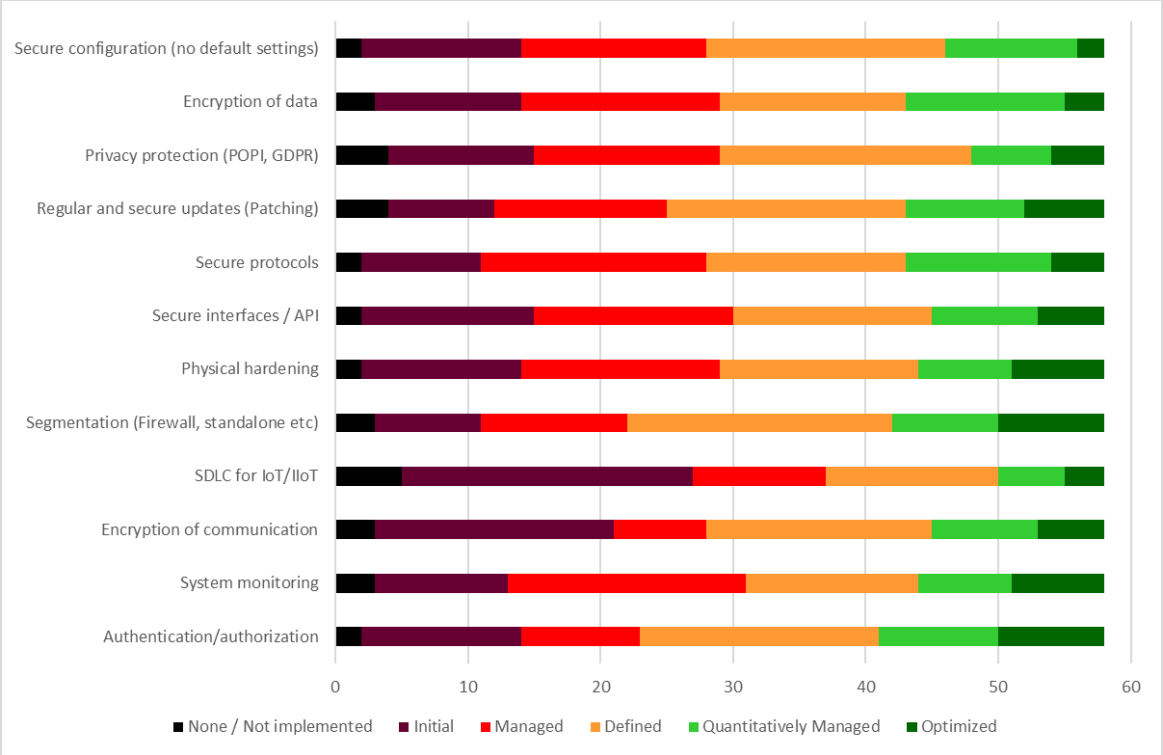


Figure 4-39: Maturity of controls to protect against the risks imposed by new IIoT

From the responses, the top 3 responses for the maturity of controls to protect against the risk imposed by new IIoT are *Segmentation (Firewall, standalone etc.)* with a mean of 2.79 (leaning towards defined - Processes characterised for the organisation and is proactive), *Authentication/authorisation* with a mean of 2.76, also leaning towards defined and third, *Regular and secure updates (Patching)* with a mean of 2.66, which is between managed (Process characterised for projects and is often reactive) and defined (Processes characterised for the organisation and is proactive).

Table 4-12: Frequency and descriptive statistics for Maturity of controls to protect against the risks imposed by new IIoT

	Authentication/authorisation	System monitoring	Encryption of communication	SDLC for IIoT	Segmentation (Firewall, standalone etc.)	Physical hardening	Secure interfaces / API	Secure protocols	Regular and secure updates (Patching)	Privacy protection (POPI, GDPR)	Encryption of data	Secure configuration (no default settings)
None / Not implemented	2	3	3	5	3	2	2	2	4	4	3	2
Initial	12	10	18	22	8	12	13	9	8	11	11	12
Managed	9	18	7	10	11	15	15	17	13	14	15	14
Defined	18	13	17	13	20	15	15	15	18	19	14	18
Quantitatively Managed	9	7	8	5	8	7	8	11	9	6	12	10
Optimised	8	7	5	3	8	7	5	4	6	4	3	2
Mean	2.76	2.55	2.41	2.00	2.79	2.59	2.50	2.62	2.66	2.41	2.52	2.48
Median	3	2	3	2	3	2.5	2	3	3	2.5	2.5	3
Mode	3	2	1	1	3	3	3	2	3	3	2	3
Std Deviation	1.41	1.38	1.41	1.34	1.37	1.36	1.31	1.25	1.37	1.30	1.30	1.20
Variance	1.98	1.90	2.00	1.79	1.89	1.86	1.73	1.57	1.88	1.69	1.69	1.45
Kurtosis	-0.9	-0.6	-1.0	-0.5	-0.6	-0.7	-0.7	-0.6	-0.6	-0.4	-0.8	-0.7
Skewness	0.0	0.2	0.2	0.5	-0.1	0.2	0.2	0.0	-0.1	0.1	0.0	0.0
Confidence Level (95.0%)	0.37	0.36	0.37	0.35	0.36	0.36	0.35	0.33	0.36	0.34	0.34	0.32
Rank (Top)	2				1				3			
Rank (Bottom)			2	1						2		

The 95% confidence intervals for the above is 0.36 for the maturity of controls related to *Segmentation (Firewall, standalone etc.)* for IIoT environment, 0.37 for the maturity of the control *Authentication/authorisation,* and 0.36 for *Regular and secure updates (Patching)*. This indicates that with 95% confidence, the population mean for the maturity of the control *Segmentation (Firewall, standalone etc.)* for IIoT environment is between 2.43 (mean – confidence = 2.79 – 0.36) to 3.15 (mean + confidence = 2.79 + 0.36), *Authentication/authorisation* with a population mean of 2.39 to 3.13, and *Regular and secure updates (Patching)* with a population mean of 2.29 to 3.02.

The bottom three responses for the maturity of controls to protect against the risk imposed by new IIoT are *SDLC for IIoT* with a mean of 2.00 which relates to managed (Process characterised for projects and is often reactive), *Encryption of communication* and *Privacy protection (POPI, GDPR)* both combined second/third with a mean of 2.41 which is between managed (Process characterised for projects and is often reactive) and defined (Processes characterised for the organisation and is proactive). Section 6.7.2.1 discusses the results further, including a unique analysis of the implications for the transport sector.

4.6 People Factors Influencing IIoT

This section relates to the research objective to determine the People factors influencing IIoT security in the transport sector of South Africa.

4.6.1 Maturity of Security Awareness for IIoT Systems

This relates to Question E1 of the questionnaire. Figure 4.40 indicates how respondents see the maturity of security awareness for their IIoT environment. To generate the descriptive statistics, the responses are rated from '0', *None / Not implemented*, '1', *Initial* to '5' *Optimised*. The results are displayed in Table 4.13.

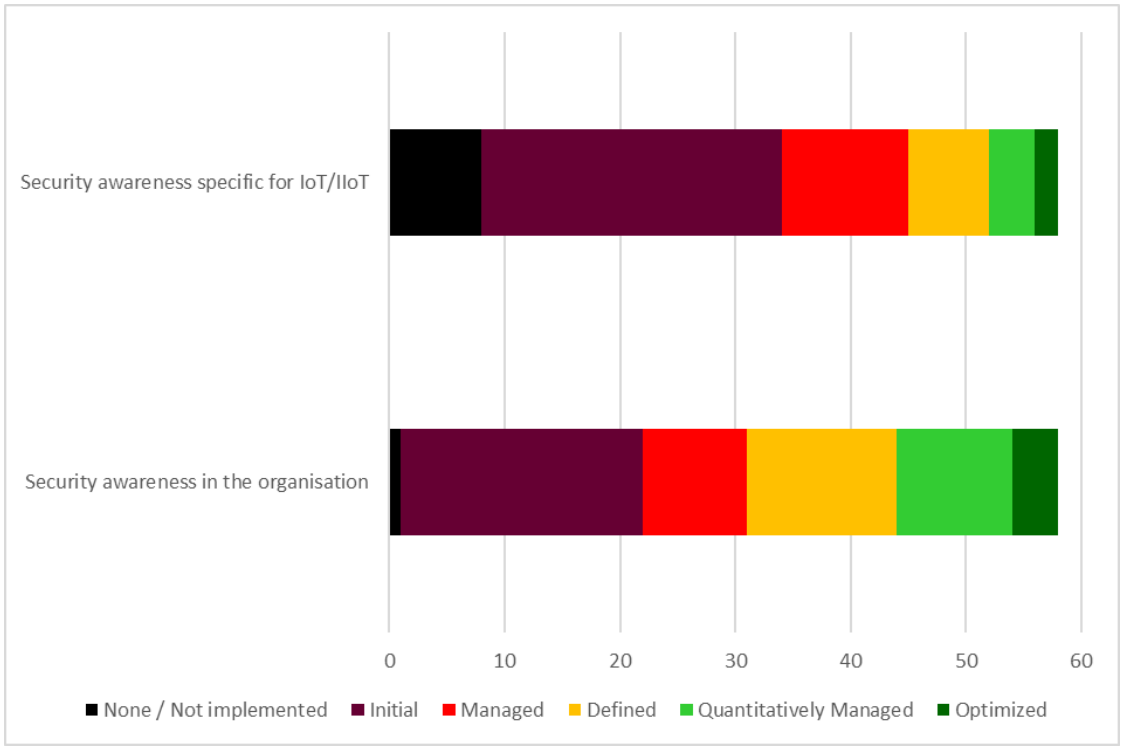


Figure 4-40: Maturity of security awareness for IIoT systems

Table 4-13: Frequency and descriptive statistics for Maturity of security awareness for IIoT environment

	Security awareness in the organisation	Security awareness specific for IIoT
None / Not implemented (0)	1	8
Initial (1)	21	26
Managed (2)	9	11
Defined (3)	13	7
Quantitatively Managed (4)	10	4
Optimised (5)	4	2
Mean	2.38	1.64
Median	2	1
Mode	1	1
Standard Deviation	1.36	1.27
Sample Variance	1.85	1.60
Kurtosis	-1.08	0.37
Skewness	0.35	0.94
Confidence Level (95.0%)	0.36	0.33

From the responses, the mean for responses of the maturity of *Security awareness in the organisation* is 2.38, which is between managed (Process characterised for projects and is often reactive) and defined (Processes characterised for the organisation and is proactive). The mean for the maturity of *Security awareness specific for IIoT* is 1.64, leaning towards managed (Process characterised for projects and is often reactive).

The 95% confidence interval for the maturity of *Security awareness in the organisation* is 0.36, and the maturity of *Security awareness specific for IIoT* is 0.33. This indicates that with 95% confidence, the population mean for the maturity of *Security awareness in the organisation* is between 2.02 (mean – confidence = 2.38 – 0.36) to 2.74 (mean + confidence = 2.38 + 0.36) and the maturity of *Security awareness specific for IIoT* with a population mean of 1.30 to 1.97.

The CMM is displayed in Figure 4.41 and Figure 4.42. Section 6.5.1 discusses the results further, including a unique analysis of the implications for the transport sector.

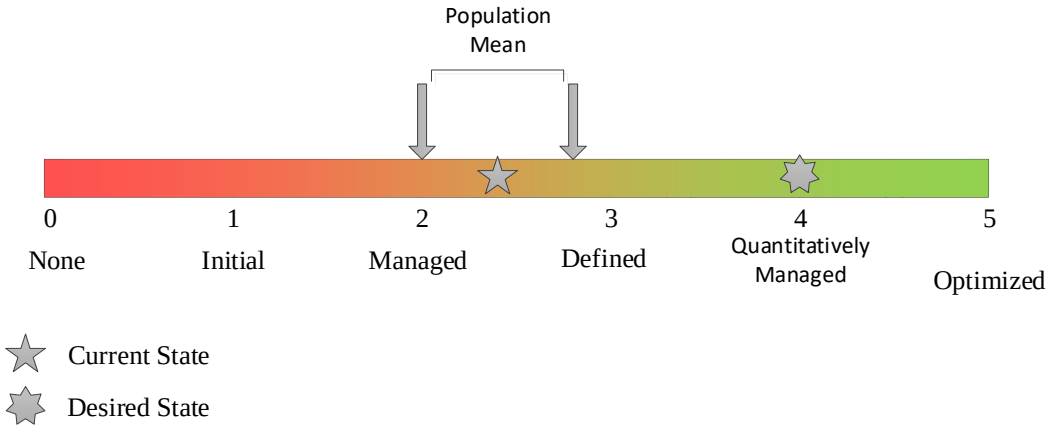


Figure 4-41: Maturity of security awareness in the organisation

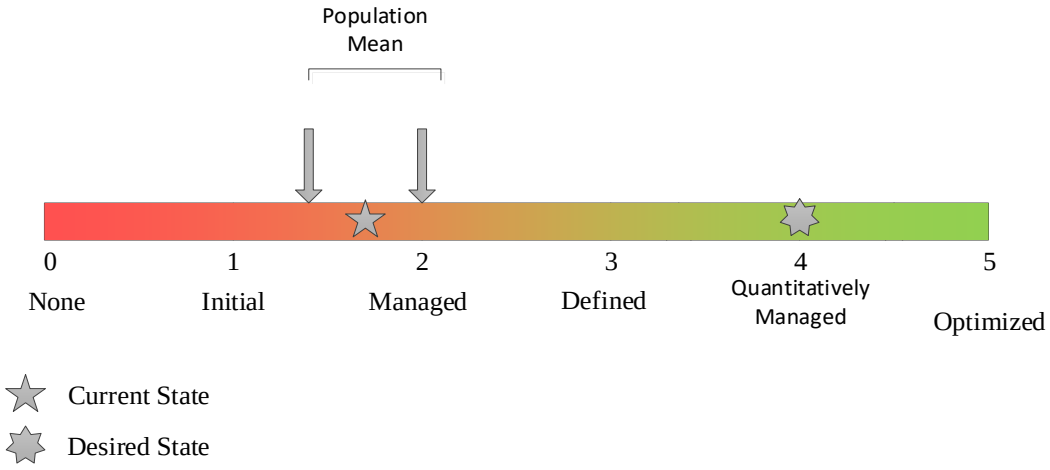


Figure 4-42: Maturity of Security awareness specific for IIoT

4.6.2 Maturity of Skills for IIoT Security

This relates to Question E2 of the questionnaire. Figure 4.43 indicates how respondents see the maturity of IIoT security skills in their organisation in the transport sector of South Africa. To generate the descriptive statistics, the responses are rated from '0', *None / Not implemented*, '1', *Initial* to '5' *Optimised*. The results are displayed in Table 4.14.

From the responses, the mean for responses of the maturity of *Employees have general security skills* for IIoT environment is 2.07, which is close to managed (Process characterised for projects and is often reactive), the mean for the maturity of *Employees have IIoT security skills* is 1.43 which is between initial (Process unpredictable, poorly controlled and reactive) and managed (Process characterised for projects and is often reactive), the mean for the maturity of *Employees are sufficiently trained to deal with IIoT security* is 1.47 also between initial and managed and the mean for the

maturity of *The organisation enable staff for security* is 1.67 all strongly leaning towards managed (Process characterised for projects and is often reactive).

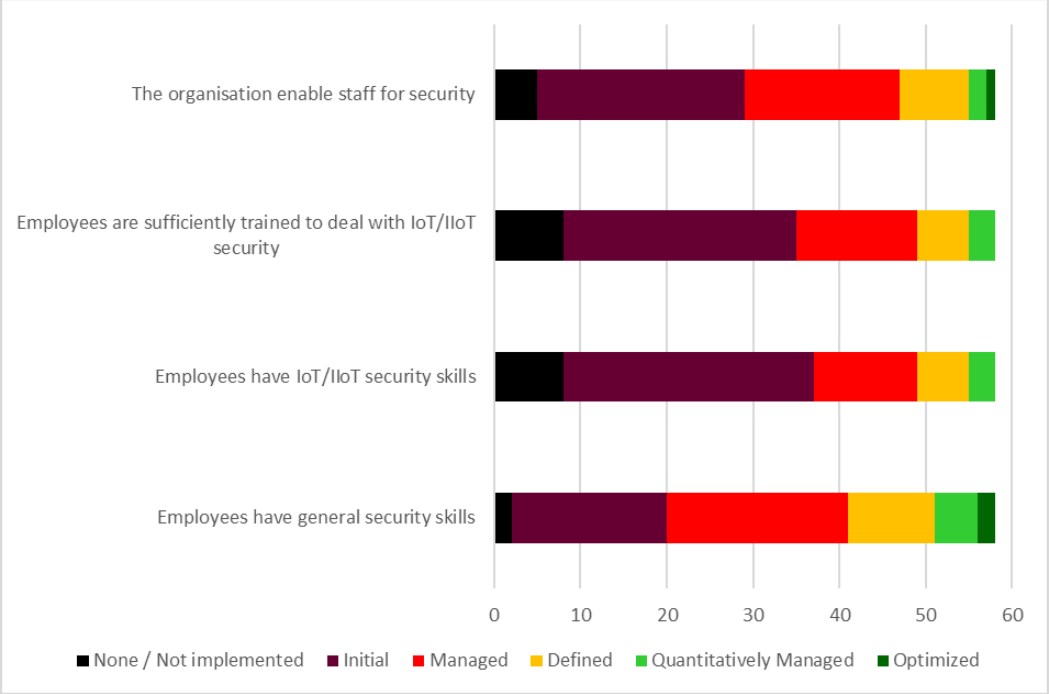


Figure 4-43: Maturity of IIoT security skills

Table 4-14: Frequency and descriptive statistics for maturity of security skills and IIoT security skills

	Employees have general security skills	Employees have IIoT security skills	Employees are sufficiently trained to deal with IIoT security	The organisation enable staff for security
None / Not implemented (0)	2	8	8	5
Initial (1)	18	29	27	24
Managed (2)	21	12	14	18
Defined (3)	10	6	6	8
Quantitatively Managed (4)	5	3	3	2
Optimised (5)	2	0	0	1
Mean	2.07	1.43	1.47	1.67
Median	2	1	1	1.5
Mode	2	1	1	1
Standard Deviation	1.14	1.03	1.03	1.05
Sample Variance	1.29	1.06	1.06	1.10

	Employees have general security skills	Employees have IIoT security skills	Employees are sufficiently trained to deal with IIoT security	The organisation enable staff for security
Kurtosis	0.15	0.38	0.24	0.86
Skewness	0.68	0.84	0.74	0.80
Confidence Level (95.0%)	0.30	0.27	0.27	0.28

The 95% confidence interval for the above is 0.30 for the maturity of *Employees have general security skills* for IIoT environment, 0.27 for both the maturity of *Employees have IIoT security skills*, and *Employees are sufficiently trained to deal with IIoT security*, and 0.28 for *The organisation enable staff for security*. This indicates that with 95% confidence, the population mean for the maturity of *Employees have general security skills* for IIoT environment is between 1.77 (mean – confidence = 2.07 – 0.30) to 2.37 (mean + confidence = 2.07 + 0.30), *Employees have IIoT security skills* with a population mean of 1.16 to 1.70, *Employees are sufficiently trained to deal with IIoT security* with a population mean of between 1.19 to 1.74, and *The organisation enable staff for security* with a population mean of 1.40 to 1.95.

The CMM is displayed in Figure 4.44 to Figure 4.47. Section 6.5.2 discusses the results further, including a unique analysis of the implications for the transport sector.

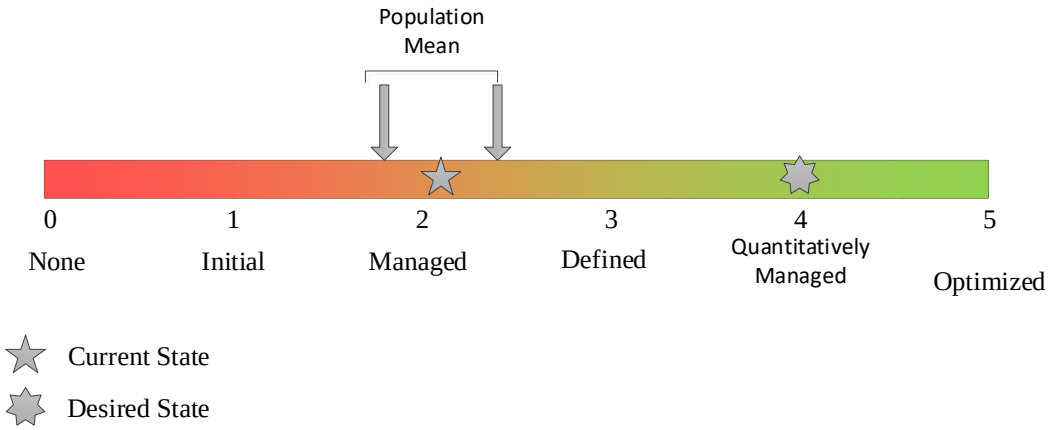


Figure 4-44: Maturity of Employees have general security skills

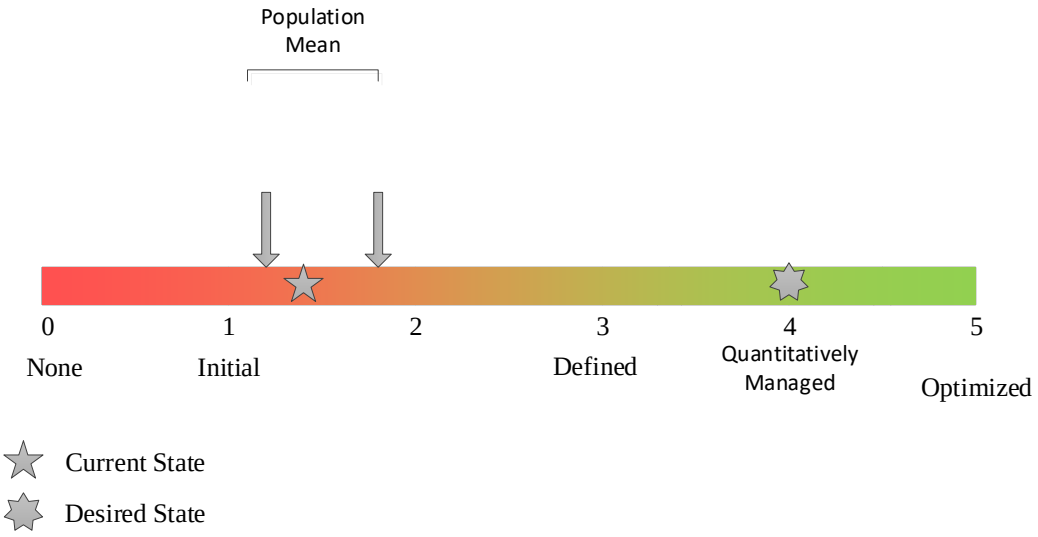


Figure 4-45: Maturity of Employees have IIoT security skills

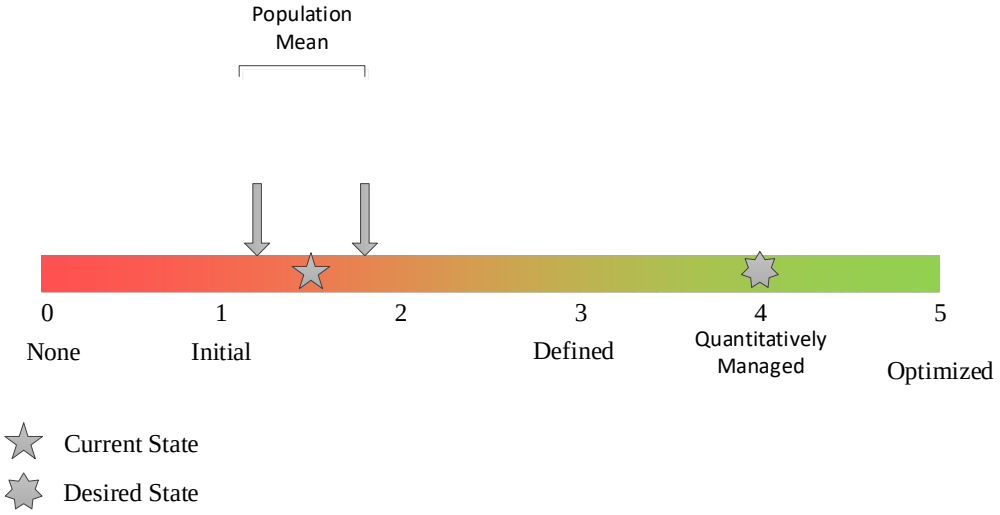


Figure 4-46: Maturity of Employees are sufficiently trained to deal with IIoT security

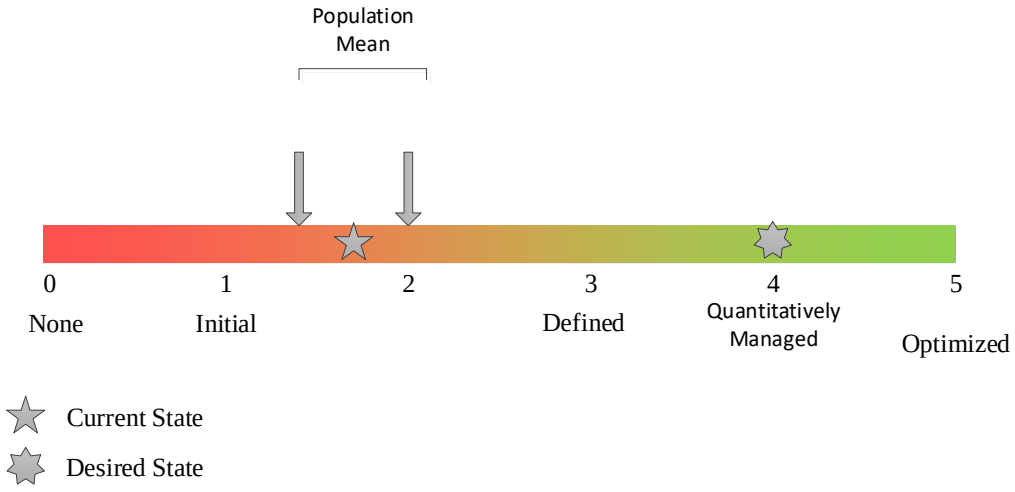


Figure 4-47: Maturity of the organisation enable staff for security

4.6.3 Maturity of Employee Engagement for IIoT Security

This relates to Question E3 of the questionnaire. Figure 4.48 indicates how respondents see the maturity of employee engagement for IIoT in their organisation in the transport sector of South Africa. To generate the descriptive statistics, the responses are rated from '0', *None / Not implemented*, '1', *Initial* to '5' *Optimised*. The results are displayed in Table 4.15

Table 4-15: Frequency and descriptive statistics for Maturity of employee engagement for IIoT security

	Engineering/OT engagement with security staff	IT engagement with security staff	Management engagement with security staff	Executive management engagement with security staff
None / Not implemented (0)	4	4	4	5
Initial (1)	21	18	20	24
Managed (2)	22	20	18	15
Defined (3)	7	11	10	10
Quantitatively Managed (4)	3	3	3	2
Optimised (5)	1	2	3	2
Mean	1.78	1.95	1.95	1.76
Median	2	2	2	1.5
Mode	2	2	1	1
Standard Deviation	1.04	1.15	1.22	1.16
Sample Variance	1.09	1.31	1.49	1.34
Kurtosis	0.85	0.37	0.35	0.62
Skewness	0.76	0.61	0.76	0.84
Confidence Level (95.0%)	0.27	0.30	0.32	0.30

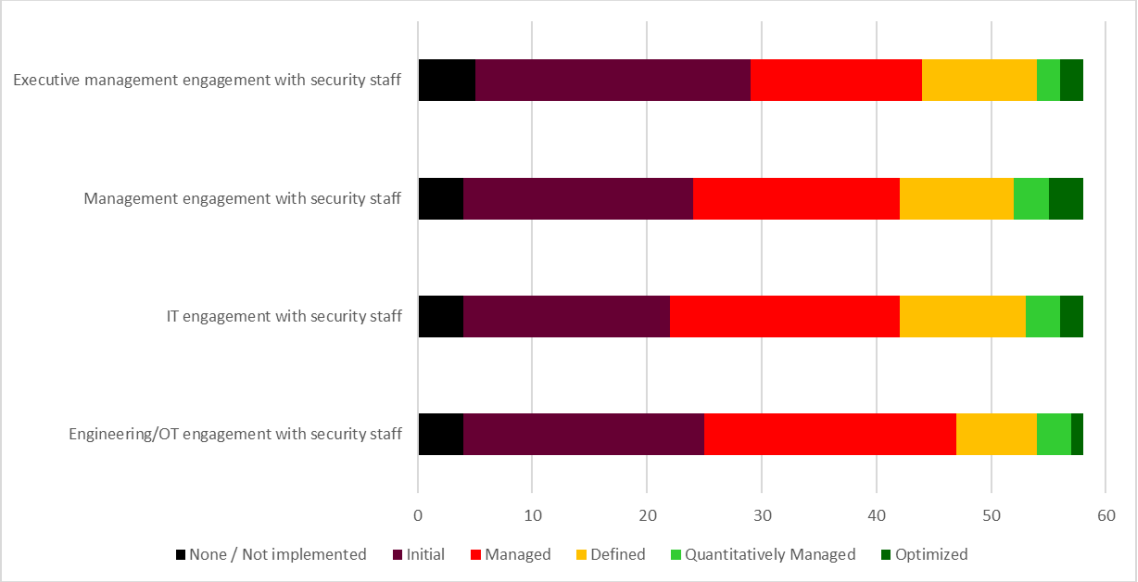


Figure 4-48: Maturity of employee engagement for IIoT security

From the responses, the mean for responses of the maturity of *Engineering/OT engagement with security staff* for IIoT environment is 1.78, which is close to managed (Process characterised for projects and is often reactive), the mean for both the maturity of *IT engagement with security staff* the maturity of *Management engagement with security staff* is 1.95 and the mean for the maturity of *Executive management engagement with security staff* is 1.76 all strongly leaning towards managed (Process characterised for projects and is often reactive).

The 95% confidence interval for the above is 0.27 for the maturity of *Engineering/OT engagement with security staff* for the IIoT environment, 0.30 for the maturity of *IT engagement with security staff*, and 0.32 for *Management engagement with security staff*, and 0.30 for *The organisation enable staff for security*. This indicates that with 95% confidence, the population mean for the maturity of *Engineering/OT engagement with security staff* for IIoT environment is between 1.50 (mean – confidence = 1.78 – 0.27) to 2.05 (mean + confidence = 1.78 + 0.27), *IT engagement with security staff* with a population mean of 1.65 to 2.25, *Management engagement with security staff* with a population mean of between 1.63 to 2.27 and *Executive management engagement with security staff* with a population mean of 1.45 to 2.06. The CMM is displayed in Figure 4.49 to Figure 4.52. Section 6.5.3 discusses the results further, including a unique analysis of the implications for the transport sector.

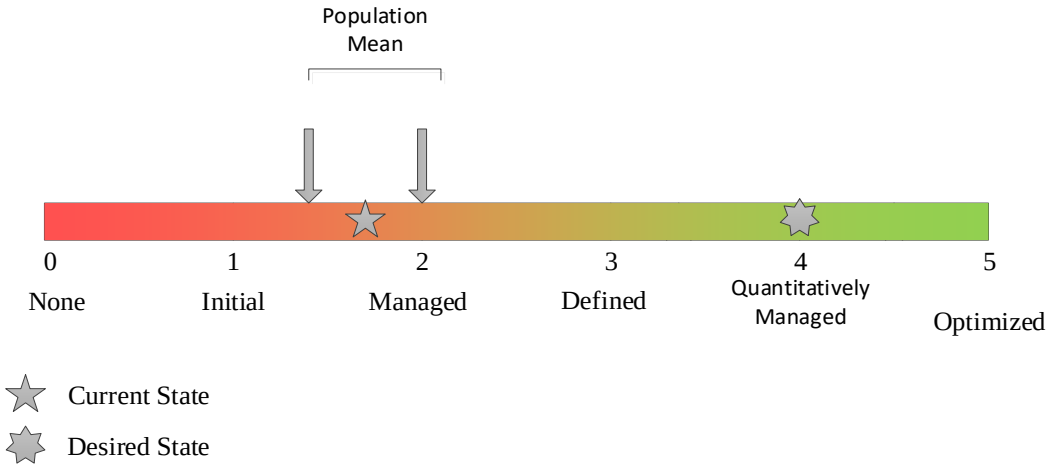


Figure 4-49: Maturity of Engineering/OT engagement with security staff

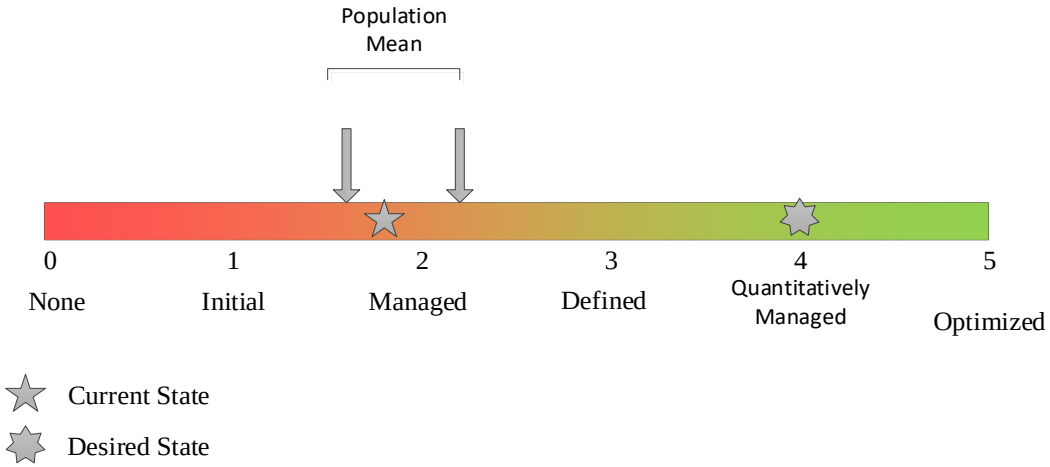


Figure 4-50: Maturity of IT engagement with security staff

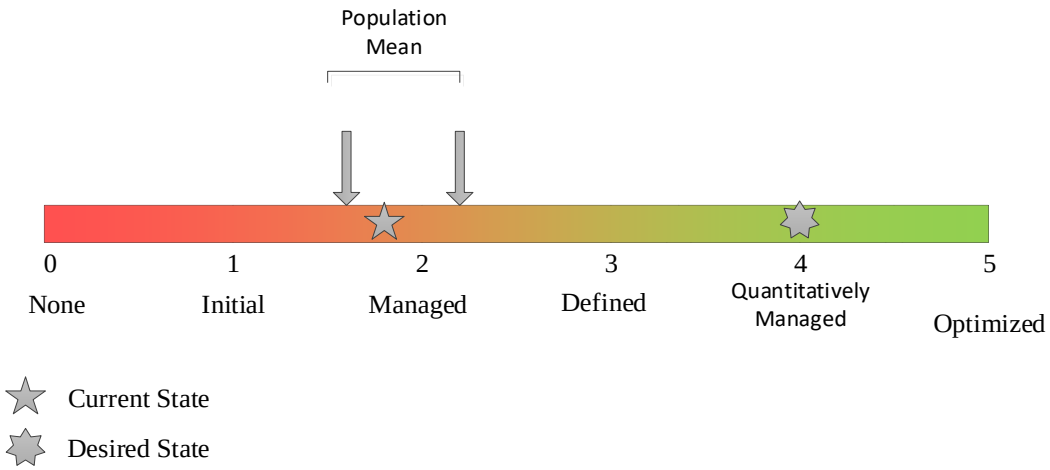


Figure 4-51: Maturity of Management engagement with security staff

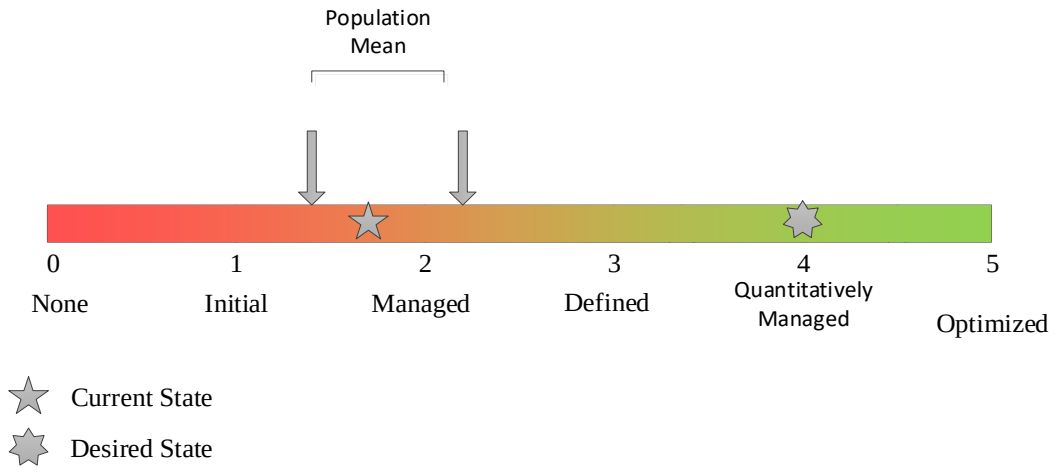


Figure 4-52: Maturity of Executive management engagement with security staff

4.6.4 Maturity of Employee Satisfaction

This relates to Question E4 of the questionnaire. Figure 4.53 indicates how respondents see the maturity of IIoT security satisfaction in their organisation in the transport sector in SA of IIoT security skill in their organisation in the transport sector of South Africa. To generate the descriptive statistics, the responses are rated from '0', *None / Not implemented*, '1', *Initial* to '5' *Optimised*. The results are displayed in Table 4.16.

From the responses, the mean for responses of the maturity of *Employees are satisfied with the organisation* for IIoT environment is 1.88, which is close to managed (Process characterised for projects and is often reactive), the mean for the maturity of *The organisation provides the tools to manage IIoT security* is 1.62 which is between initial (Process unpredictable, poorly controlled and reactive) and managed (Process characterised for projects and is often reactive), the mean for the maturity of *Employees energy* is 1.74 and *Employees productivity* is at 1.78 leaning towards managed (Process characterised for projects and is often reactive).

Table 4-16: Frequency and descriptive statistics for Maturity of Employee satisfaction

	Employees are satisfied with the organisation	The organisation provides the tools to manage IIoT security	Employee' s energy	Employee' s productivity
None / Not implemented (0)	4	4	5	3
Initial (1)	21	30	23	24

	Employees are satisfied with the organisation	The organisation provides the tools to manage IIoT security	Employee' s energy	Employee' s productivity
Managed (2)	21	16	22	22
Defined (3)	7	4	3	5
Quantitatively Managed (4)	0	0	0	0
Optimised (5)	5	4	5	4
Mean	1.88	1.62	1.74	1.78
Median	2	1	2	2
Mode	1	1	1	1
Standard Deviation	1.24	1.17	1.24	1.14
Sample Variance	1.55	1.36	1.53	1.30
Kurtosis	1.30	2.81	2.04	2.40
Skewness	1.14	1.62	1.38	1.42
Confidence Level (95.0%)	0.33	0.31	0.33	0.30

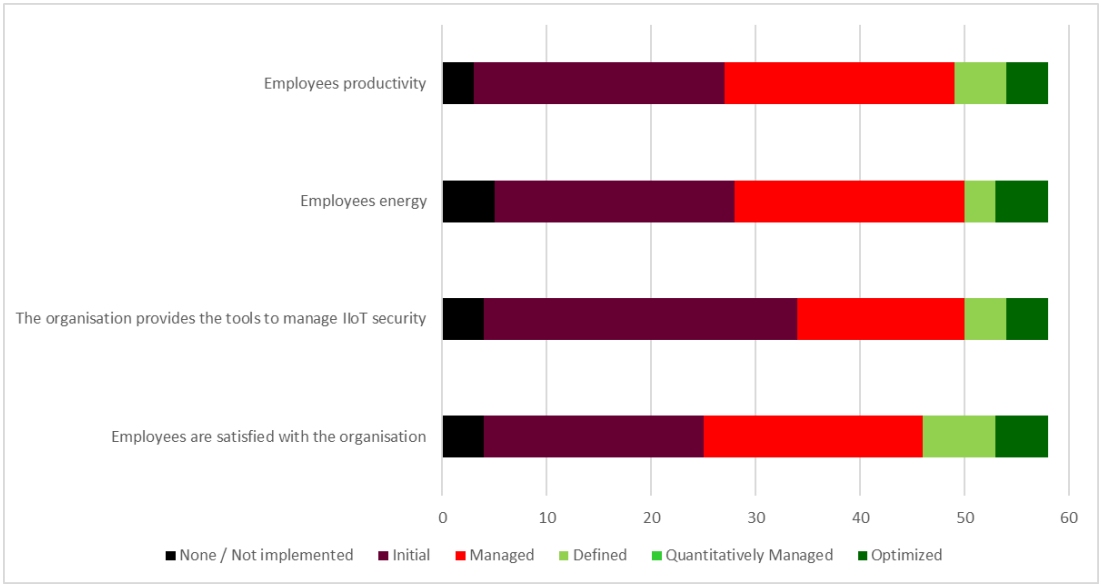


Figure 4-53: Maturity of Employee satisfaction

The 95% confidence interval for the above is 0.33 for the maturity of *Employees are satisfied with the organisation* for IIoT environment, 0.31 the maturity of *The organisation provides the tools to manage IIoT security*, 0.33 for the maturity of *Employee's productivity*, and 0.30 for *Employee's energy*. This indicates that with 95% confidence, the population mean for the maturity of *Employees are satisfied with the organisation* for IIoT environment is between 1.55 (mean – confidence = 1.88 – 0.33) to 2.21 (mean + confidence = 1.88 + 0.33), *The organisation provides the tools to manage IIoT security* with

a population mean of 1.31 to 1.93, *Employees energy* with a population mean of between 1.42 to 2.07 and *Employees productivity* with a population mean of 1.48 to 2.08.

The CMM is displayed in Figure 4.54 to Figure 4.57. Section 6.5.4 discusses the results further, including a unique analysis of the implications for the transport sector.

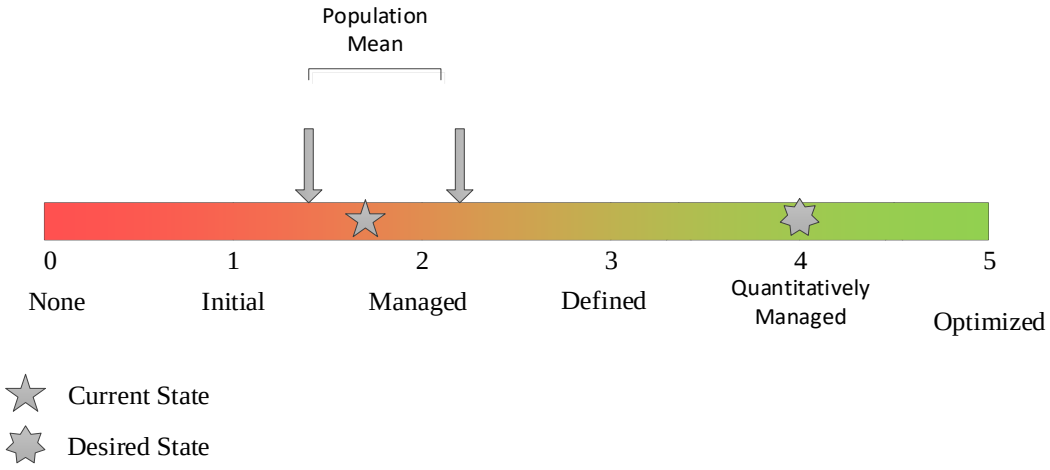


Figure 4-54: Maturity of Employees are satisfied with the organisation

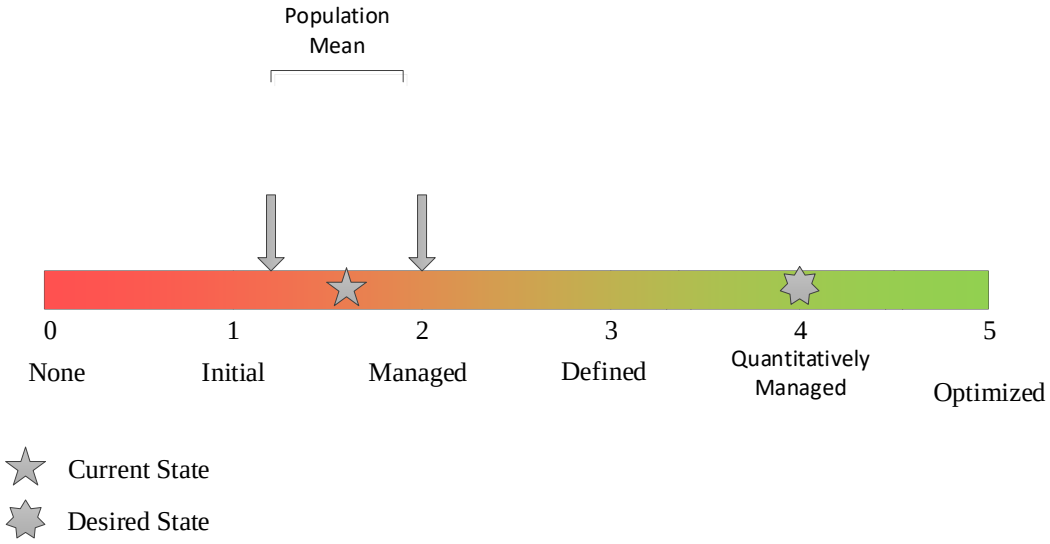


Figure 4-55: Maturity of the organisation provides the tools to manage IIoT security

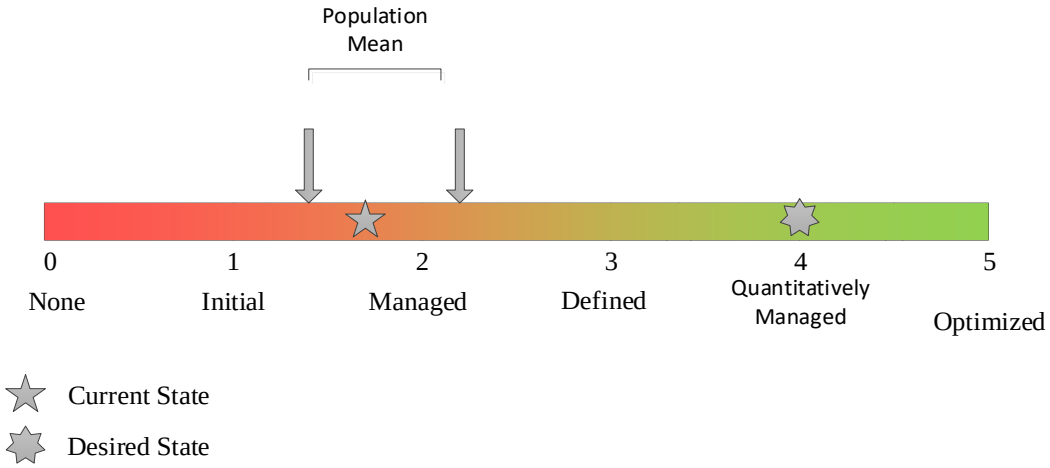


Figure 4-56: Maturity of Employees' energy

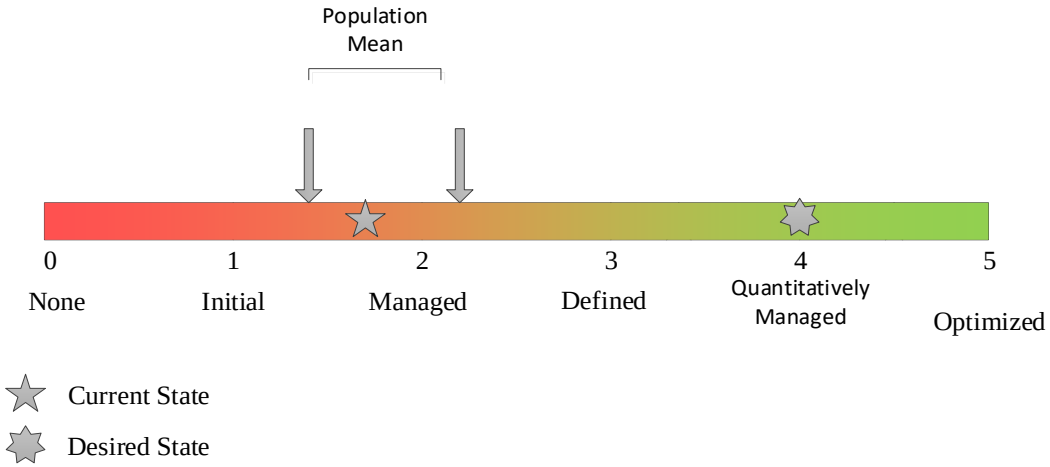


Figure 4-57: Maturity of Employees' productivity

4.7 Correlation between Factors

The correlation between the technological, organisational, procedural and people factors is calculated using Pearson correlation. Temizel et al. (2011) outlined that the Pearson correlation is a prominent statistical method utilised to gauge the relationship strength between two variables. Pearson's correlation coefficient maintains its popularity and widespread usage within statistical analyses as the leading correlation coefficient (Temizel et al., 2011). The Pearson correlation can range between -1 and 1, with 1 denoting a perfect match, 0 representing no correlation, and -1 indicating a perfect negative correlation; the Pearson correlation coefficient is computed by dividing the variables' covariance by their standard deviations. Self-correlation has been removed for convenience; hence, there is no symmetry.

4.7.1 Correlation between Technological and Organisational Factors (Architecture)

4.7.1.1 Correlation between Technological (threats) and Organisational Factors

Table 4-17: Partial Correlation table between Technological (threats) and Organisational factors

	DDoS	Cyber espionage	Denial-of-sleep	Man-in-the-Middle attack	Remote Access	Signal jamming attack
Risk appetite for IIoT	-0.44	-0.46	-0.50	-0.41	-0.30	-0.38
Governance processes for IIoT	-0.46	-0.46	-0.41	-0.49	-0.47	-0.51

Legend

Colour	Explanation
Strong	Strong correlation where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5.
Moderate	Moderate correlation where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5
None	None where no correlation exists.

From the partial correlation matrices in Table 4.17, the full list is displayed in Appendix B, it is observed that there are two strong correlations (where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5) between the technological (threat) and organisational factors. A strong negative correlation is between *Denial-of-sleep* and *Risk appetite for IIoT* (-0.5) and a strong negative correlation between *Signal jamming attack* and *Governance processes for IIoT* (-0.51). There is also some moderate correlation (where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3

to 0.5) between the technological (threat) and organisational factors. The top five moderate negative correlations are as follows: *Man-in-the-Middle attack* and *Governance processes for IIoT* (-0.49), *Remote Access* and *Governance processes for IIoT* (-0.47), *DDoS* and *Risk appetite* for IIoT (-0.46), *Cyber espionage* and *Risk appetite* for IIoT (-0.46), *Cyber espionage* and *Governance processes for IIoT* (-0.46) and *Man-in-the-Middle attack* and *Risk appetite for IIoT* (-0.44). Section 6.6.1.1 discusses the results further, including a unique analysis of the implications for the transport sector.

4.7.1.2 Correlation between Technological (vulnerabilities) and Organisational Factors

From the partial correlation matrices in Table 4.18, the full list is displayed in Appendix B, it is observed that there is no strong correlation (where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5) between any of the technological (Vulnerabilities) and organisational factors. There is only one moderate correlation (where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5), namely between *Insecure Default Settings* and *Employees supporting IIoT* (0.3). Section 6.6.1.2 discusses the results further, including a unique analysis of the implications for the transport sector.

Table 4-18: Partial Correlation table between Technological (vulnerabilities) and Organisational factors

	Insecure Default Settings
Employees supporting IIoT	**0.3**

Legend

Colour	**Explanation**
Strong	Strong correlation where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5.
Moderate	Moderate correlation where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5
None	None where no correlation exists.

4.7.1.3 Correlation between Technological (risks) and Organisational Factors

It is observed that there is no strong correlation (where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5) or moderate correlation (where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5 between any of the technological (Risks) and organisational factors. The tables are displayed in Appendix B. Section 6.6.1.3 discusses the results further, including a unique analysis of the implications for the transport sector.

4.7.2 Correlation between Technological and Procedural Factors (Enabling & Support)

4.7.2.1 Correlation between Technological (threats) and Procedural Factors

From the partial correlation matrices in Table 4.19, it is observed that there is only one strong correlation (where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5) between one of the technological (threat) and procedural factors. The negative correlation is

between *Denial-of-sleep* and *Risk assessment for IIoT* (-0.50). There is also some moderate negative correlation (where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5) between the technological (threat) and procedural factors. The top five are *DDoS* and *Risk assessment for IIoT* (-0.4), *Cyber espionage* and *Risk assessment for IIoT* (-0.4), *Man-in-the-Middle attack* and *Risk assessment for IIoT* (-0.4), *Signal jamming attack* and *Risk assessment for IIoT* (-0.4), *Denial-of-sleep* and *Governance processes for IIoT* (-0.35). Section 6.6.2.1 discusses the results further, including a unique analysis of the implications for the transport sector.

Table 4-19: Correlation table between Technological (threats) and Procedural factors

	Threats													
	DDoS	**Insider and privilege misuse**	**Cyber espionage**	**Web Application attacks**	**Malware**	**Natural disaster / environmental**	**Crime ware**	**Denial-of-sleep**	**Ransomware**	**Man-in-the-Middle attack**	**Remote access**	**Signal jamming attack**	**BlueBorne Attack (Bluetooth)**	**Other**
Organisation has an incident response plan	0.0	0.2	0.1	0.3	0.3	0.3	0.2	0.0	0.2	0.1	0.2	0.1	0.2	0.1
Incident response plan address IIoT risk	-0.2	0.1	-0.2	0.0	0.1	0.1	0.0	-0.3	0.0	-0.2	0.0	-0.1	-0.1	-0.1
Risk assessment for IIoT	-0.4	-0.2	-0.4	-0.2	-0.1	-0.1	-0.2	-0.5	-0.3	-0.4	-0.3	-0.4	-0.3	-0.1
General security policies/ procedures implemented	-0.1	-0.1	0.1	0.1	0.1	0.0	0.1	0.0	0.0	-0.1	0.0	0.0	0.2	0.0
IIoT security policies/ procedures/controls implemented	-0.2	0.0	-0.1	-0.2	-0.1	0.0	-0.2	-0.3	-0.2	-0.3	-0.2	-0.2	-0.1	-0.2

	Threats													
	DDoS	**Insider and privilege misuse**	**Cyber espionage**	**Web Application attacks**	**Malware**	**Natural disaster / environmental**	**Crime ware**	**Denial-of-sleep**	**Ransomware**	**Man-in-the-Middle attack**	**Remote access**	**Signal jamming attack**	**BlueBorne Attack (Bluetooth)**	**Other**
Governance processes for IIoT	-0.2	-0.1	-0.1	-0.2	-0.1	0.0	0.0	-0.3	-0.3	-0.3	-0.2	-0.2	-0.1	-0.1
Control framework for IIoT	-0.1	0.0	-0.1	-0.2	-0.1	-0.1	-0.1	-0.3	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2

Legend

Colour	Explanation
Strong	Strong correlation where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5.
Moderate	Moderate correlation where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5
None	None where no correlation exists.

4.7.2.2 Correlation between Technological (vulnerabilities) and Procedural Factors

From the partial correlation matrices in Table 4.20, the full list is displayed in Appendix B, it is observed that there is no strong correlation between the technological (vulnerabilities) and procedural factors.

There is a moderate correlation between *Use of insecure or outdated components* and *Organisation has an incident response plan* (0.4), *No privacy protection* and *Organisation has an incident response plan* (0.3), *Insecure Network Services* and *Organisation has an incident response plan* (0.3) and *Insecure Data Transfer and Storage* and *Organisation has an incident response plan* (0.3).

There are also some moderate negative correlations between the following: *Misconfiguration* and *Governance processes for IIoT* (-0.3) and *Misconfiguration* and *Control framework for IIoT* (-0.3).

Table 4-20: Correlation table between Technological (vulnerabilities) and Procedural factors

	Misconfiguration	*No privacy protection*	*Insecure Network Services*	*Use of insecure or outdated components*	*Insecure Data Transfer and Storage*
Organisation has an incident response plan	0.1	0.3	0.3	0.4	0.3
Governance processes for IIoT	-0.3	-0.1	-0.1	-0.2	0.0
Control framework for IIoT	-0.3	-0.1	-0.1	-0.2	0.0

Legend

Colour	**Explanation**
Strong	Strong correlation (where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5.
Moderate	Moderate correlation where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5
None	None where no correlation exists.

Section 6.6.2.2 discusses the results further, including a unique analysis of the implications for the transport sector.

4.7.2.3 Correlation between Technological (risks) and Procedural Factors

It is observed that there is no strong correlation (where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5) between any of the technological (risk) and procedural factors.

There is one moderate correlation (where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5) that is negative between *Physical asset damage* and *IIoT security policies/procedures/controls implemented* (-0.3), and one moderate positive correlation between *Data corruption or loss of data integrity* and *Organisation has an incident response plan* the full list is displayed in Appendix B. Section 6.6.2.3 discusses the results further, including a unique analysis of the implications for the transport sector.

4.7.3 Correlation between Technological and People Factors (Human Factors)

4.7.3.1 Correlation between Technological (threats) and People Factors

It is observed that there is no strong correlation or moderate correlation between any of the technological (threat) and people factors, the correlation matrices are displayed in Appendix B.

4.7.3.2 Correlation between Technological (vulnerabilities) and People Factors

From the partial correlation matrices in Table 4.22, the full list is displayed in Appendix B, it is observed that there is no strong correlation between any of the technological (vulnerabilities) and people factors.

There are, however, also some moderate negative correlations between the technological (vulnerabilities) and people factors. The top five are: *Misconfiguration* and *Employees have IIoT security skills* (-0.4), *Misconfiguration* and *Employees are sufficiently trained to deal with IIoT security* (-0.4), *Lack of Physical Hardening* and *Employees have IIoT security skills* (-0.3), *Lack of Physical Hardening* and *Employees are sufficiently trained to deal with IIoT security* (-0.3), and *Lack of Physical Hardening* and *Employees energy* (-0.4). Section 6.6.3.2 discusses the results further, including a unique analysis of the implications for the transport sector.

Table 4-21: Correlation table between Technological (vulnerabilities) and People factors

	Misconfiguration	**Lack of Physical Hardening**
Employees have IIoT security skills	-0.4	-0.3
Employees are sufficiently trained to deal with IIoT security	-0.4	-0.3
Employee's energy	-0.1	-0.4

Legend

Colour	**Explanation**
Strong	Strong correlation where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5.
Moderate	Moderate correlation where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5
None	None where no correlation exists.

4.7.3.3 Correlation between Technological (risks) and People Factors

It is observed that there is no strong correlation or moderate correlation between any of the technological (risk) and people factors, the full list is displayed in Appendix B.

4.7.4 Correlation between Organisational and Procedural Factors (Governing)

Table 4-22: Correlation table between Organisational and Procedural factors

	Employees supporting IIoT	Security staff	IIoT security staff	Cybersecurity roadmap / strategy supporting IIoT	Risk assessment for IIoT	Governance processes for IIoT	Innovative culture in the organisation	Security culture in the organisation	Senior / Executive understanding of IIoT security risks
Organisation has an incident response plan	0.3	0.3	0.2	0.3	0.3	0.2	0.3	0.3	0.3
Incident response plan address IIoT risk	0.3	0.4	0.3	0.4	0.5	0.4	0.4	0.5	0.5
Risk assessment for IIoT	0.4	0.5	0.4	0.7	1.0	0.9	0.8	0.7	0.7
General security policies/procedures implemented	0.1	0.3	0.4	0.4	0.3	0.3	0.3	0.3	0.2
IIoT security policies/procedures/controls implemented	0.2	0.4	0.4	0.4	0.4	0.5	0.3	0.5	0.4
Governance processes for IIoT	0.2	0.2	0.4	0.5	0.5	0.5	0.3	0.4	0.4
Control framework for IIoT	0.2	0.2	0.4	0.5	0.4	0.5	0.2	0.4	0.4

Legend

Colour	Explanation
Strong	Strong correlation (where the correlation coefficient, r, is greater or equal than 0.5 or less than -0.5.
Moderate	Moderate correlation where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5
None	None where no correlation exists.

From the partial correlation matrices in Table 4.23, it is observed that there is a strong correlation between the following organisational and procedural factors. The top five are: *Cybersecurity roadmap/strategy supporting IIoT* and *Risk assessment for IIoT* (0.7), *Governance processes for IIoT* and *Risk assessment for IIoT* (0.9), *Innovative culture in the organisation* and *Risk assessment for IIoT* (0.8), *Security culture in the organisation* and *Risk assessment for IIoT* (0.7), and *Senior / Executive understanding of IIoT security risks* and *Risk assessment for IIoT* (0.7). Section 6.6.4 discusses the results further, including a unique analysis of the implications for the transport sector.

4.7.5 Correlation between Organisational and People Factors (Culture)

From the partial correlation matrices in Table 4.24, it is observed that there are three strong correlations between the organisational and people factors. They are *Security staff and IT engagement with security staff* (0.5), *Risk assessment for IIoT* and *Security awareness specific for IIoT (0.5)*, and *Governance processes for IIoT* and *Security awareness specific for IIoT* (0.5).

Table 4-23: Correlation table between Organisational and People factors

	Employees supporting IIoT	**Security staff**	**IIoT security staff**	**Cybersecurity roadmap / strategy supporting IIoT**	**Risk assessment for IIoT**	**Governance processes for IIoT**	**Innovative culture in the organisation**	**Security culture in the organisation**	**Senior / Executive understanding of IIoT security risks**
Security awareness in the organisation	0.2	0.1	0.1	0.2	0.2	0.2	0.2	0.2	0.2
Security awareness specific for IIoT	0.1	0.3	0.3	0.4	0.5	0.5	0.4	0.4	0.4
Employees have general security skills	0.2	0.0	0.0	0.2	0.2	0.1	0.1	0.1	0.1
Employees have IIoT security skills	0.1	0.3	0.3	0.4	0.4	0.4	0.3	0.3	0.3
Employees are sufficiently trained to deal with IIoT security	0.1	0.3	0.4	0.4	0.4	0.4	0.3	0.4	0.4
The organisation enable staff for security	0.3	0.2	0.2	0.3	0.2	0.2	0.2	0.2	0.2
Engineering/OT engagement with security staff	0.1	0.4	0.2	0.4	0.4	0.4	0.4	0.3	0.4
IT engagement with security staff	0.3	0.5	0.3	0.2	0.4	0.3	0.3	0.4	0.4
Management engagement with security staff	0.3	0.3	0.1	0.1	0.3	0.3	0.3	0.3	0.4
Executive management engagement with security staff	0.2	0.1	0.2	0.2	0.1	0.1	0.1	0.2	0.2
Employees are satisfied with the organisation	0.1	0.0	0.0	0.2	0.1	0.1	0.2	0.2	0.2
The organisation provides the tools to manage IIoT security	0.3	0.4	0.3	0.3	0.3	0.3	0.3	0.3	0.3
Employee’s energy	0.2	0.2	0.2	0.2	0.1	0.1	0.2	0.2	0.2
Employee’s productivity	0.3	0.2	0.2	0.3	0.2	0.2	0.2	0.2	0.2

Legend

Colour	Explanation
Strong	Strong correlation where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5.
Moderate	Moderate correlation where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5
None	None where no correlation exists.

Section 6.6.5 discusses the results further, including a unique analysis of the implications for the transport sector.

4.7.6 Correlation between Procedural and People Factors (Emergence)

From the partial correlation matrices in Table 4.25, it is observed that there are strong correlations between the procedural and people factors, the top three are:

Combined first, *Control framework for IIoT* and *Employees are sufficiently trained to deal with IIoT security* (0.65), and *Governance processes for IIoT* and *Security awareness specific for IIoT* (0.65), second *Control framework for IIoT* and *Security awareness specific for IIoT* (0.54) and thirdly, *IIoT security policies/procedures/controls implemented* and *The organisation provides the tools to manage IIoT security* (0.62). There are also several moderate correlations as displayed in Table 4.25.

Table 4-24: Correlation between Procedural and People factors

	Organisation has an incident response plan	Incident response plan address IIoT risk	Risk assessment for IIoT	General security policies/procedures implemented	IIoT security policies/procedures/controls implemented	Governance processes for IIoT	Control framework for IIoT
Security awareness in the organisation	0.60	0.30	0.20	0.46	0.38	0.36	0.30
Security awareness specific for IIoT	0.38	0.53	0.49	0.48	0.59	0.65	0.64
Employees have general security skills	0.57	0.25	0.17	0.44	0.28	0.31	0.34
Employees have IIoT security skills	0.28	0.44	0.39	0.39	0.52	0.60	0.60
Employees are sufficiently trained to deal with IIoT security	0.30	0.47	0.36	0.43	0.54	0.60	0.65
The organisation enable staff for security	0.44	0.29	0.17	0.22	0.34	0.40	0.44
Engineering/OT engagement with security staff	0.42	0.56	0.43	0.44	0.57	0.50	0.55

	Organisation has an incident response plan	Incident response plan address IIoT risk	Risk assessment for IIoT	General security policies/procedures implemented	IIoT security policies/procedures/controls implemented	Governance processes for IIoT	Control framework for IIoT
IT engagement with security staff	0.41	0.50	0.36	0.32	0.43	0.34	0.39
Management engagement with security staff	0.54	0.54	0.30	0.22	0.44	0.35	0.35
Executive management engagement with security staff	0.41	0.27	0.09	0.16	0.39	0.29	0.25
Employees are satisfied with the organisation	0.52	0.31	0.11	0.39	0.36	0.22	0.19
The organisation provides the tools to manage IIoT security	0.37	0.58	0.34	0.38	0.62	0.42	0.38
Employee's energy	0.41	0.49	0.14	0.24	0.49	0.35	0.33
Employee's productivity	0.45	0.47	0.24	0.31	0.54	0.45	0.42

Legend

Colour	Explanation
Strong	Strong correlation where the correlation coefficient, r, is greater or equal than 0.5 or less than or equal to -0.5.
Moderate	Moderate correlation where the correlation coefficient, r, is between -0.5 and -0.3 or 0.3 to 0.5
None	None where no correlation exists.

Section 6.6.6 discusses the results further, including a unique analysis of the implications for the transport sector.

4.8 Reliability

The questions listed in Table 4.26 contained questions for which the Cronbach Alpha coefficient could be calculated. Questions A1 – A6, B2, B5, B6, C3, C4, D3, D4, D5, and D6 contained one variable, and Cronbach Alpha's coefficient could not be calculated. The internal consistency is considered reliable when the Cronbach Alpha coefficient is greater than 0.6; where the Cronbach Alpha coefficient is between 0.6 and 0.8, the internal consistency is considered acceptable. Where the Cronbach Alpha coefficient is between 0.8 and 0.9, the internal consistency is good, and where the Cronbach Alpha coefficient is greater than 0.9, the internal consistency is excellent. Overall, the internal consistency ranges from reliable to excellent. This shows great reliability of the data.

Table 4-25: Cronbach Alpha for each question

Question	Cronbach Alpha	Description
B1 Existing and new threats introduced by IIoT	0.934561598	Internal consistency is excellent
B3 Vulnerabilities related to IIoT	0.957159368	Internal consistency is excellent
B4 Risks of unsecured IIoT devices (impact)	0.945291106	Internal consistency is excellent
B4 Risks of unsecured IIoT devices (likelihood)	0.946163131	Internal consistency is excellent
C1 Size and structure	0.847185564	Internal consistency is *good*
C2 Security strategy	0.937914893	Internal consistency is excellent
D1 Maturity of incident response	0.797563832	Internal consistency is *acceptable* bordering *good*
D2 Maturity of IIoT policies, procedures, frameworks, standards	0.941271178	Internal consistency is excellent
D7 Maturity of controls to protect against the risks imposed by new IIoT	0.962749014	Internal consistency is excellent
E1 Maturity of security awareness for IIoT	0.645612372	Internal consistency is *reliable* bordering *acceptable*
E2 Maturity of skills for IIoT security	0.888867614	Internal consistency is *good*
E3 Maturity of employee engagement for IIoT	0.854464959	Internal consistency is *good*
E4 Maturity for IIoT employee satisfaction	0.895690357	Internal consistency is *good*

4.9 Summary

The chapter presented the results from the quantitative data analysis using a questionnaire. The demographics of the respondent are discussed. The top three threats (existing and new) likely to be introduced by IIoT are discussed together with the top vulnerabilities and risks related to the transport sector of South Africa. These form the technological factors. The organisational factors influencing IIoT in the transport sector of SA are discussed and include the size and structure of the organisation, the security strategy, responsibility of the security of IIoT as well as the maturity of the security of IIoT.

The study discussed the procedural factors influencing IIoT in the transport sector and explored the results related to the maturity of the incident response for IIoT, IIoT policies, procedures, control frameworks, threat intelligence and the maturity of controls to adequately protect the IIoT environment against the risks. The study discussed the top three frameworks used by the respondents to govern and secure their IIoT environments and are used to guide the selection of the documents in the next chapter.

The maturity of the people factors influencing IIoT in the transport sector are discussed namely the security awareness for IIoT, the skills required to successfully support IT, general security, and security of IIoT systems. The results of the employee engagement and the employee satisfaction were also discussed. The correlations between the technological, organisational, procedural and people factors are determined.

The results from this chapter (quantitative analysis) are used to determine the factors influencing IIoT in South Africa's transport sector and as input to developing a cybersecurity framework. The results are triangulated to the qualitative analysis in the next chapter.

The next chapter analyses secondary data and document analysis (qualitative analysis).

Chapter 5 Secondary Data and Document Analysis

5.1 Introduction

In the previous chapter, the analysis of the quantitative data was shown. This chapter presents the analysis of qualitative data and documents. The documentary methods to collect the data from best practices, standards, and frameworks, are analysed using descriptive statistics and summarised to address the Research Objectives mentioned in Section 1.5.2.

Data from Shodan is obtained, sanitised, and analysed. The document analysis is performed by selecting existing frameworks, security alert reports and trends. The data from the documents is then divided into pre-determined categories, coded, and summarised. Figure 5.1 is a graphical representation of the outline of this chapter and its overall structure. The output from the document analysis will be triangulated to the quantitative data and used as input to develop the cybersecurity framework for IIoT in the South African transport sector.

This chapter presents the analysis of secondary data and documents.

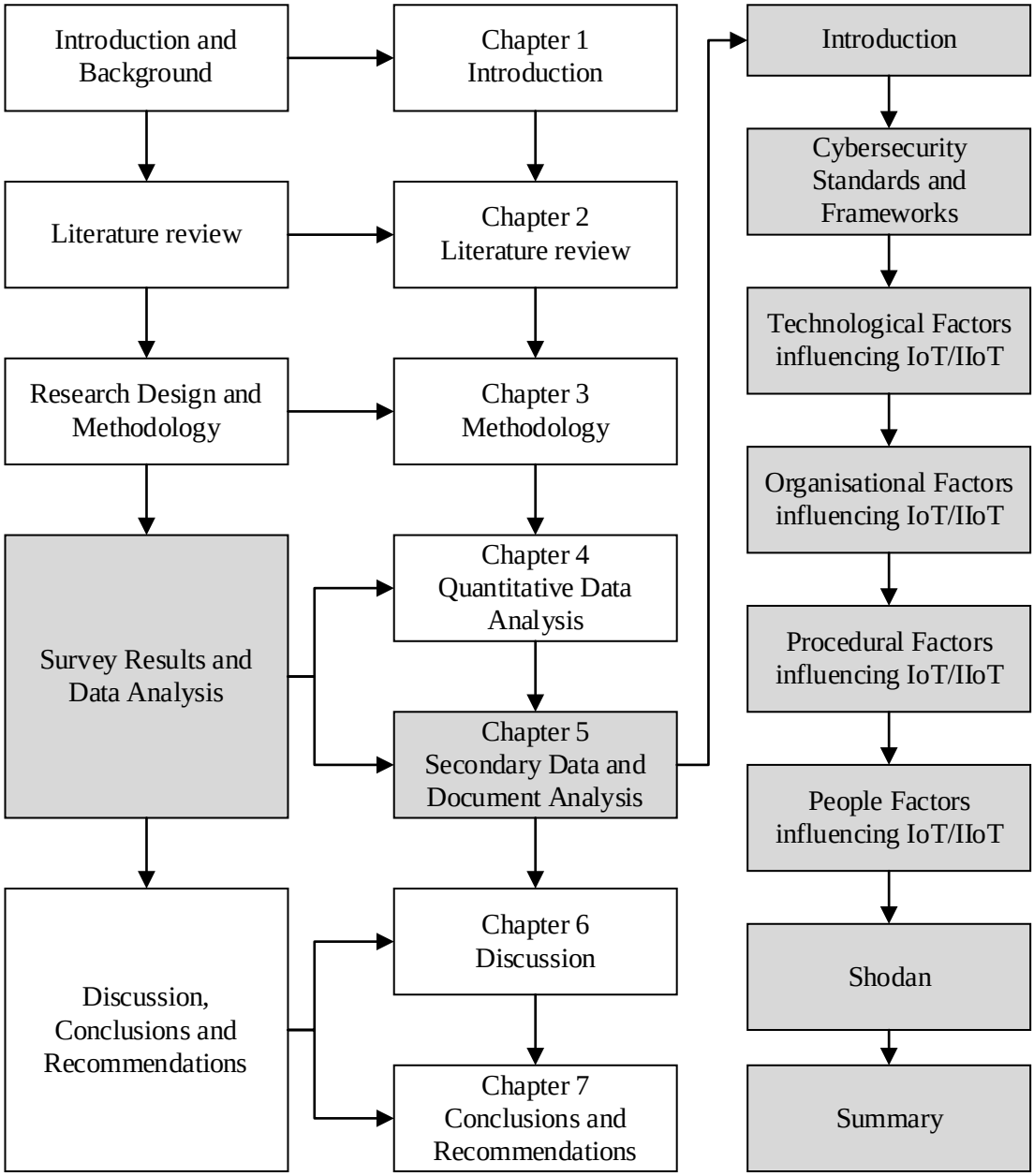


Figure 5-1: Graphical representation of Chapter 5 outline

5.2 Cybersecurity Standards and Frameworks

The sample for the document analysis is chosen by selecting common and freely available cybersecurity standards, frameworks and best practices related to Information security, IoT, IIoT and ICS/SCADA.

5.2.1 Framework Selection

Qualitative analysis of cybersecurity standards, frameworks and best practices is conducted through thematic and content analysis using the software NVivo. Table 5.1 represent the documents considered by professional bodies based on the topic's relevance and the relationship to the results from the

Questionnaire in Section 4.5.3. Based on the IIoT relevance and percentage of responses from the questionnaires, the following five documents are selected, these include:

- NIST: IR.8228 Consideration for Managing IoT Cybersecurity and Privacy Risks.
- Microsoft: Internet of Things security best practices.
- Cloud Security Alliance: Security Guidance for Early Adopters of the Internet of Things (IoT).
- IIC: Industrial Internet of Things, Volume G4: Security Framework and
- Online Trust Alliance: IoT Trust Framework.

The analysis provides contents in terms of frequency for the significant words related to the research objectives mentioned in Chapter 3, Section 1.5.2 and the documents selected. The prevalent themes in the documents are provided via thematic analysis, indicating the relationships between the various documents and research objectives.

Table 5-1: List of documents considered for document analysis

Published by	Framework	Questionnaire response	Relevance	Selected (Y/N)
ISACA	COBIT 2019	Yes (65%)	No mention of IoT or IIoT	No
ISO	ISO27001	Yes (46%)	No mention of IoT or IIoT	No
NIST	NIST IR.8228 Consideration for Managing IoT Cybersecurity and Privacy Risks	Yes (38%)	Yes, IoT or IIoT mentioned 339 times	Yes
ITIL	ITIL v4	Yes (35%)	No mention of IoT or IIoT	No
IEEE IoT	P2413 – Standard for an Architectural Framework for the Internet of Things (IoT)	Yes (23%)	Yes* Not freely available	No
Microsoft	Internet of Things security best practices	Yes (20%)	Yes, IoT or IIoT mentioned 308 times	Yes
Cloud Security Alliance	Security Guidance for Early Adopters of the Internet of Things (IoT)	Yes (18%)	Yes, IoT or IIoT mentioned 407 times	Yes
IIC	Industrial Internet of Things, Volume G4: Security Framework	Yes (9%)	Yes, IoT or IIoT mentioned 228 times	Yes
TOGAF	TOGAF	Yes (6%)	No mention of IoT or IIoT	No
Online Trust Alliance	IoT Trust Framework	Yes (6%)	Yes, IoT or IIoT mentioned 26 times	Yes
Alliance for internet of things innovation	AIOTI WG07 AIOTI WG09	Yes (5%)	Yes, IoT mentioned 22 times	No

Published by	Framework	Questionnaire response	Relevance	Selected (Y/N)
Open connectivity foundation	OCF Security FAQ, and OCF 1.1.1 Security Specification	Yes (3%)	Yes, IoT or IIoT mentioned 7 times	No
IT4IT	IT4IT	Yes (2%)	No mention of IoT or IIoT	No
US Department of Homeland Security (DHS)	Securing the Internet of Things	Yes (2%)	Yes, IoT or IIoT mentioned 86 times	No
International Electrotechnical Commission (IEC)	ISO/IEC 30165:2021	No	Yes, IoT or IIoT mentioned 41 times	No
Object Management Group	DDS-Security	No	No	No
Thread Group	Thread 1.1 Specification	No	No	No
Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	No	Yes, IoT or IIoT mentioned 153 times	No
Groupe Spécial Mobile Association (GSMA)	GSMA IoT Security Guidelines	No	Yes, IoT or IIoT mentioned 332 times	No
U.S. Food and Drug Administration (FDA)	Postmarket Management of Cybersecurity in Medical Devices	No	No	No

Figure 5.2 provides a cluster analysis, using Pearson's correlation, of the documents based on word similarity. Pearson's correlation is used as linear relationships between documents are calculated. Pearson's correlation measures the strength and direction of the linear relationship between each pair of the documents. Pearson correlation is used as it has been identified as a more accurate method for assessing correlations (Chetty, 2022). There are two main clusters; the first comprises documents that specifically address the security of the Industrial Internet of Things, with the prominent document being the "Industrial Internet of Things Volume G4 Security Framework". The second cluster comprises of documents focusing on the broader Internet of Things security.

Within the cluster, the document "Security Guidance for Early Adopters of the Internet of Things" exhibits the closest similarity to the document "Microsoft – Security Best Practices for Internet of Things (IoT)". The document "NIST IR.8228 Consideration for Managing IoT Cybersecurity and Privacy Risks" follows closely behind.

This analysis demonstrates the distinct focus on Industrial IoT security within one cluster while the other encompasses more general IoT security topics. It also highlights the proximity and similarity between specific documents, indicating their shared concerns and insights regarding IoT security best

practices.

Figure 5-2: Sources clustered by word similarity

5.2.2 Document Analysis using Coding, Nodes and Word Trees

NVivo software is used for document analysis and coding. NVivo is a software tool designed to aid researchers in systematically managing, analysing, and visualising qualitative data, such as documents, individually and systematically (Dhakal,2022).

A crucial aspect of a qualitative data analysis tool is its role in coding. Coding entails meticulously examining the gathered data to discern significant themes, sub-themes, emerging patterns, concepts, categories, and other valuable insights within the research. (Hai-Jew, n.d.). Coding the datasets entails labelling and categorising sections of data within the documents. This enables users to create data categories from single or multiple sources, incorporating attributes and values and allowing for the mapping of thematic data to case data. By utilising these coding, classification, and mapping tools, researchers can enhance the organisation of their data, enabling them to query, analyse, draw conclusions, and validate findings across all units of analysis more effectively. To perform thematic coding in NVivo, a portion of text from a source document, such as a framework, is selected and assigned a tag using a node (Dhakal,2022).

To determine the extent to which the factors influence IIoT cybersecurity, nodes are created to link the references to the relevant factors in the five documents analysed via NVivo. A node is a collection of references about a specific theme, case, or relationship. References are assigned by coding sources to a node. All the references can be seen in one place when the node is open.

The word frequency for each research objective and the factors influencing them are visualised. For each infographic, the larger the word, the higher the frequency of occurrence.

Word trees expand the words derived from the words prevalent in the nodes. Word trees enable the visualization of the context preceding and following specific words or phrases (Dhakal,2022). These are the main phrases from the documents, and they demonstrate basic security principles applied to IIoT as well. This will guide the development of the control framework in Section 6.7.

5.3 Technological Factors Influencing IIoT Cybersecurity

The following section evaluates the technological factors influencing IIoT cybersecurity. To assess the impact of technological factors on IIoT cybersecurity, nodes were established to connect references to these factors across the five (5) documents analysed using NVivo. Table 5.2 summarises the count and percentage coverage (%) of nodes for each technological factor (Risk, Threat, and Vulnerabilities) per document analysed. The percentage coverage shows the extent of source content coded at the specified node. It is calculated based on the percentage of characters coded in text selections and the percentage of page area coded in region selections at the node (Nvivo, 2021). From here, we can see most of the nodes coded under technological factors are from the document 'Industrial Internet of Things Volume G4 Security Framework'.

Table 5-2: Summary of Technological factors

	Technological factors		
Document	**Risk**	**Threat**	**Vulnerabilities**
Industrial Internet of Things Volume G4 Security Framework	141 (0.29%)	193 (0.46%)	71 (0.16%)
IoT Trust Framework	6 (0.27%)	10 (0.38%)	3 (0.18%)
Microsoft – Security Best practices for Internet of Things (IoT)	54 (0.57%)	49 (0.48%)	10 (0.10%)
NIST	26 (0.21%)	3 (0.03%)	14 (0.14%)
Security Guidance for Early Adopter of the Internet of Things	54 (0.44%)	73 (0.49%)	69 (0.45%)

The overall node frequency per word for technological factors is displayed in Table 5-3 and visualised in Figure 5.3. We noted the word 'unauthorised' are most prevalent with a frequency of 43, 'data' and 'tampering' with a frequency of 36 each, 'attacks' with 35 and 'privacy' with 34. The meaning of these is further unpacked under each of the technological factors.

Table 5-3: Overall node frequency for Technological factors

	Technological				
Document	**Unauthorised**	**Data**	**Tampering**	**Attacks**	**Privacy**
Industrial Internet of Things Volume G4 Security Framework	30 (0.04%)	20 (0.01%)	10 (0.01%)	25 (0.02%)	6 (0,01%)
IoT Trust Framework	2 (0.06%)	2 (0.02%)		1 (<0.01%)	0
Microsoft – Security Best practices for Internet of Things (IoT)	2 (0,01%)	7 (0.02%)	23 (0.11%)	1 (<0.01%)	3 (0,01%)
NIST					10 (0,03%)
Security Guidance for Early Adopter of the Internet of Things	9 (0.04%)	7 (0.02%)	3 (0.01%)	8 (0.02%)	15 (0,04%)
TOTAL	**43**	**36**	**36**	**35**	**34**

Figure 5-3: Overall word frequency for technological factors

Next, the work frequency for each technological factors linked to the research objective is analysed and visualised.

5.3.1 Existing and New Threats due to IIoT

The word frequency for the factor, ‘Existing and new threats due to IIoT’, is visualised in Figure 5.4 and summarised in Table 5.4. The word ‘unauthorised’ is most prevalent. This is due to any unauthorised action being a threat. The words following this in prevalence are: ‘attacks’, ‘malicious’, ‘tampering’ and ‘access’. To better understand what ‘unauthorised’ threats and what ‘attacks’ are the factors, a text search on the node, ‘threats’ under technological factors is conducted, and the results are displayed in a word tree for each of the most frequent words.

Figure 5-4: Visualisation of the word frequency for Existing and new threats due to IIoT

Table 5-4: Table of the word frequency for Existing and new threats due to IIoT

	Existing and new threats due to IIoT				
Document	**Unauthorised**	**Attacks**	**Malicious**	**Tampering**	**Access**
Industrial Internet of Things Volume G4 Security Framework	28 (0.04%)	22 (0.02%)	18 (0.02%)	10 (0.01%)	10 (0.01%)
IoT Trust Framework	2 (0.06%)	1 (0.02%)	1 (0.02%)		2 (0.03%)
Microsoft – Security Best practices for Internet of Things (IoT)		1 (0.02%)	4 (0.02%)	13 (0.06%)	3 (0.01%)
NIST					1 (0.01%)
Security Guidance for Early Adopter of the Internet of Things	5 (0.02%)	7 (0.02%)	3 (0.01%)	3 (0.01%)	3 (0.01%)
TOTAL	**35**	**31**	**26**	**26**	**19**

The text search on the node, ‘existing and new threats due to IIoT’ under technological factors, is conducted for the word ‘unauthorised’, and the results of the word tree are displayed in Figure 5.5. From here, we can see that the factors for existing and new threats due to IIoT are unauthorised access, unauthorised changes, endpoints, unauthorised parties, unauthorised use, and unauthorised users.

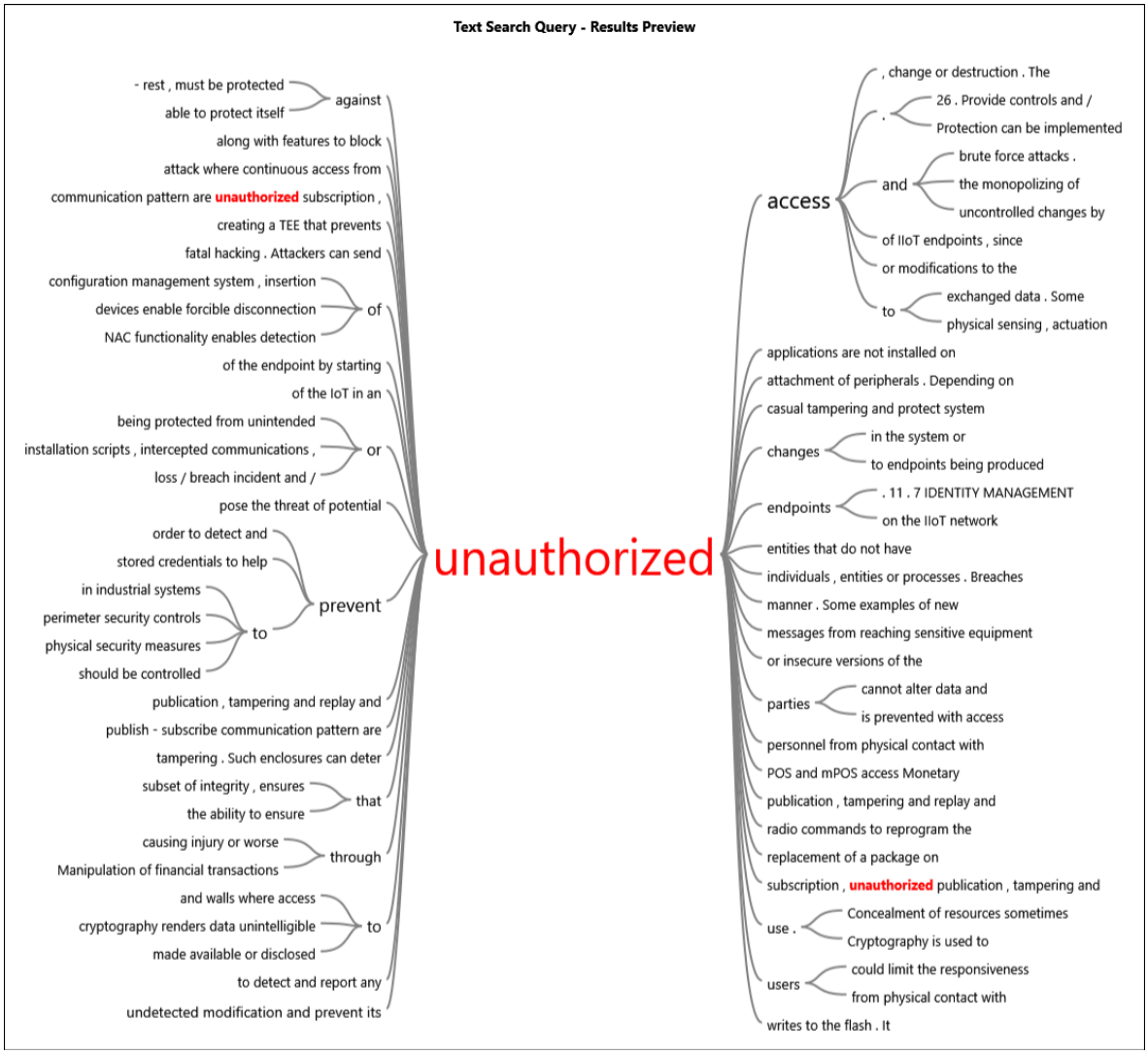


Figure 5-5: Word tree for 'unauthorised' under the threat node

The text search on the node, 'existing and new threats due to IIoT' under technological factors, is conducted for the words 'attacks', 'malicious', 'tampering' and 'access'. The word tree results are displayed in Appendix C (Figure C1 – Figure C4).

From the analysis of the frequency of nodes for the factor, 'Existing and new threats due to IIoT', we can conclude that the most prevalent words are:

- **Unauthorised:** unauthorised access, unauthorised changes, unauthorised endpoints, unauthorised parties, unauthorised use, and unauthorised users.
- **Attacks:** physical attacks, network attacks, attacks against software, 0-day attacks, denial of service attacks, brute force attacks and memory attacks.
- **Malicious:** malicious activity, malicious attacks/attackers, malicious code, malicious changes/alterations, and malicious applications.
- **Tampering:** physical tampering, data/information tampering, spoofing tampering, and other tampering.

- **Access:** unauthorised access, unwanted/improper access, privileged access, remote access, and physical access.

Section 6.2.1 discusses the results further, including a unique analysis of the implications for the transport sector.

5.3.2 Vulnerabilities

The word frequency for the factor, 'vulnerabilities', is visualised in Figure 5.6 and summarised in Table 5.5. The word 'legacy' is again most prevalent because many legacy systems in ICS/SCADA environments are incredibly vulnerable as most are no longer supported with security patches. The words following this in prevalence are: 'security', 'insecure', 'lack', and 'protocols'. To better understand what 'insecure' vulnerability relates to and what 'security' are the factors, a text search on the node, 'vulnerabilities' under technological factors is conducted, and the results are displayed in a word tree for each of the most frequent words.

Figure 5-6: Visualisation of the word frequency for Vulnerabilities to IIoT

Table 5-5: Table of the word frequency for Vulnerabilities to IIoT

	Vulnerabilities				
Document	**Legacy**	**Security**	**Insecure**	**Lack**	**Protocol**
Industrial Internet of Things Volume G4 Security Framework	14 (<0.01%)	9 (<0.01%)	7 (<0.01%)	1 (<0.01%)	5 (<0.01%)
IoT Trust Framework					

	Vulnerabilities				
Document	**Legacy**	**Security**	**Insecure**	**Lack**	**Protocol**
Microsoft – Security Best practices for Internet of Things (IoT)	1 (<0.01%)				
NIST				3 (<0.01%)	
Security Guidance for Early Adopter of the Internet of Things		4 (<0.01%)	3 (<0.01%)	4 (<0.01%)	2 (<0.01%)
TOTAL	**15**	**13**	**10**	**8**	**7**

The text search on the node 'vulnerabilities' under technological factors is conducted for the word 'legacy', and the results of the word tree are displayed in Figure 5.7. From here, we can see that the factors for vulnerabilities to IIoT are legacy endpoints/devices, legacy communications/protocols, legacy industrial or OT systems, and legacy network segments.

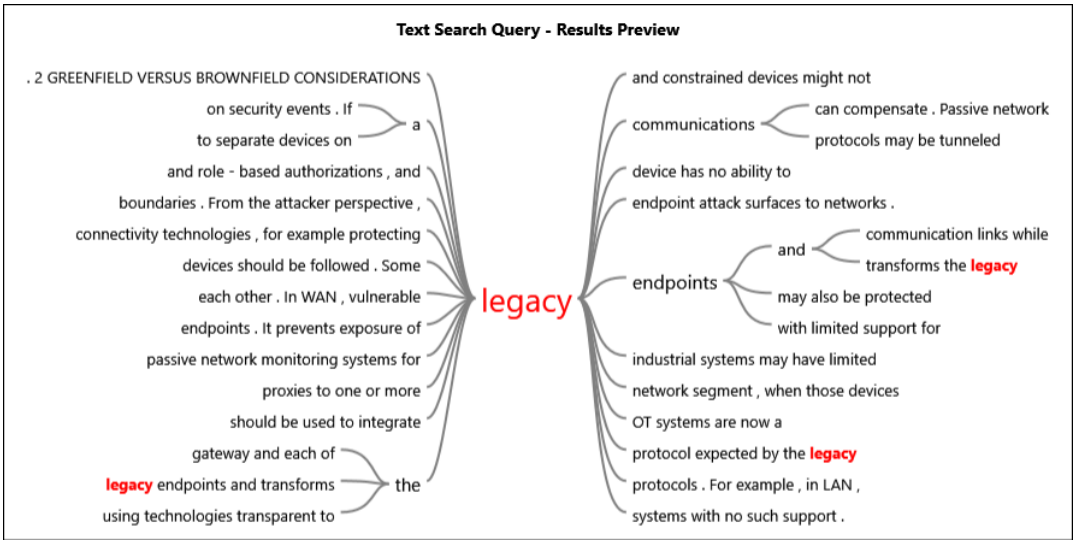


Figure 5-7: Word tree for 'legacy' under the vulnerability node

The text search on the node 'vulnerabilities' under technological factors is conducted for the words 'security', 'insecure', 'lack', and 'protocols'. The word tree results are displayed in Appendix C (Figure C5 – Figure C8)

From the analysis of the frequency of nodes for the factor 'vulnerabilities', we can conclude that the most prevalent words are:

- **Legacy**: legacy endpoints/devices, legacy communications/protocols, legacy industrial or OT system, and legacy network segment.
- **Security**: poor physical security, bypass security, out-of-date security, lack of security controls, security vulnerabilities/weaknesses, and incorrect security configurations.

- **Insecure**: insecure cloud, insecure encryption protocols, insecure IoT platforms/gateways, insecure interfaces (e.g., mobile, web and API), insecure network services, insecure software, and insecure operating systems / redundant operating systems.
- **Protocols**: legacy protocols and misconfigured NAT/port mapping protocols.
- **Lack**: lack of transport encryption, lack of standards for authentication, lack of security engineering, lack of interfaces, lack of inventory capabilities, and lack of management features.

Section 6.2.2 discusses the results further, including a unique analysis of the implications for the transport sector.

5.3.3 Risks

The word frequency for the factor, 'risk', is visualised in Figure 5.8 and summarised in Table 5.6. The word 'privacy' is most prevalent because the primary objective of IIoT is to provide valuable data and valuable business insides where the privacy of such data is a huge concern. The words following this in prevalence are: 'data', 'safety', 'systems', and 'physical'. To gain a clearer understanding of what 'privacy' risk and what 'data', 'safety', 'systems', and 'physical' are factors, a text search on the node, 'risks' under technological factors are conducted, and the results displayed in a word tree for each of the most frequent words.

Figure 5-8: Visualisation of the word frequency for Technological Risks to IIoT

Table 5-6: Table of the word frequency for Technological Risks to IIoT

	Risks				
Document	**Privacy**	**Data**	**Safety**	**Information**	**Physical**
Industrial Internet of Things Volume G4 Security Framework	5 (<0.01%)	9 (<0.01%)	16 (<0.01%)	4 (<0.01%)	7 (<0.01%)
IoT Trust Framework		2 (0.02%)			
Microsoft – Security Best practices for Internet of Things (IoT)	3 (<0.01%)	7 (0.02%)	1 (<0.01%)	4 (0.02%)	2 (<0.01%)
NIST	10 (0.03%)		2 (<0.01%)		4 (0.02%)
Security Guidance for Early Adopter of the Internet of Things	14 (0.03%)	2 (0.01%)	1 (<0.01%)	8 (0.03%)	3 (<0.01%)
TOTAL	**32**	**20**	**20**	**16**	**16**

The text search on the node ‘risks’ under technological factors is conducted for the word ‘privacy’, and the results of the word tree are displayed in Figure 5.9. From here, we can see the factors for risks to IIoT are privacy risk/risks, security privacy, privacy concerns, privacy data, privacy ramifications and user privacy.

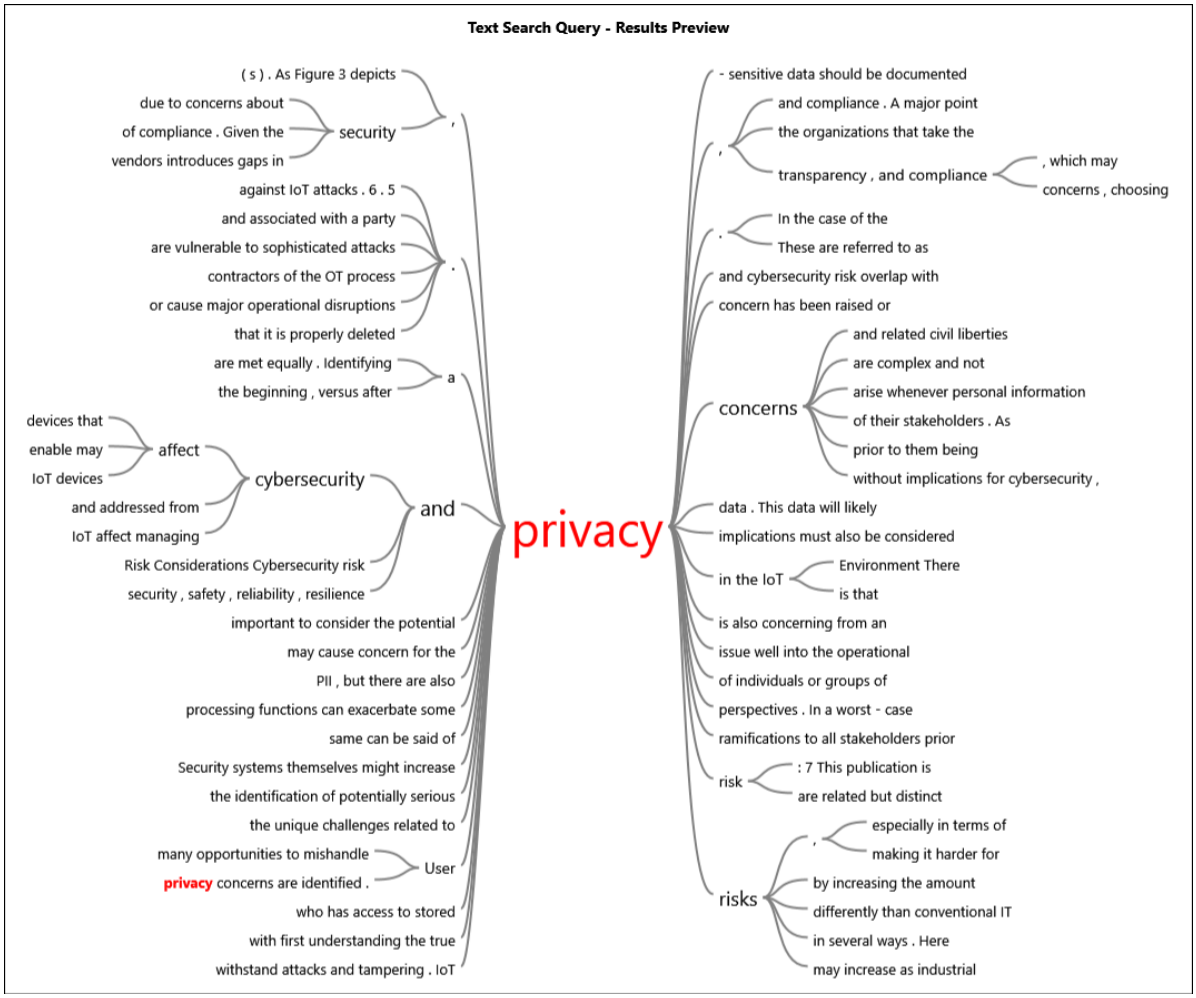


Figure 5-9: Word tree for 'privacy' under the risk node

The text search on the node 'risks' under technological factors is conducted for the words 'data', 'safety', 'systems', and 'physical'. The word tree results are displayed in Appendix C (Figure C9 – Figure C12.

From the analysis of the frequency of nodes for the factor 'risks', we can conclude that the most prevalent words are:

- **Privacy:** privacy risk/risks, security privacy, privacy concerns, privacy data, privacy ramifications and user privacy.
- **Data:** sensitive data (privacy and disclosure), data to unauthorised parties, data exfiltration and leaks, false/bad data, personal data, tampering with data, and data loss/breach.
- **Safety:** human safety, safety issues, communications safety, safety policies, safety regulations/considerations/consequences/implications, safety threats, and safety risks.
- **Information:** personal information, sensitive information, critical information, private information, information modification, information disclosure, information modification, and stolen information.

- **Physical:** physical access, physical world, physical attacks, tampering physically with IoT devices, physical control equipment, physical injury, physical interference, physical infrastructure, physical security, and physical processes.

Section 6.2.3 discusses the results further, including a unique analysis of the implications for the transport sector.

5.4 Organisational Factors Influencing IIoT Cybersecurity

The following section evaluates the organisational factors influencing IIoT cybersecurity. To determine the extent to which the organisational factors influence IIoT cybersecurity, nodes are created to link the references to organisational factors in the five (5) documents analysed via NVivo. Table 5.7 summarises the count and percentage (%) of nodes for each organisation factor (Size and structure, Cybersecurity strategy, Risk appetite, Innovativeness culture, Security Culture, and Senior executive engagement with security) per document analysed. From here, we can see most of the nodes coded under organisational factors are from the document 'Industrial Internet of Things Volume G4 Security Framework'.

Table 5-7: Summary of Organisational factors

	Organisational					
Document	**Size and structure**	**Cybersecurity strategy**	**Risk appetite**	**Innovativeness culture**	**Security Culture**	**Senior executive engagement with security**
Industrial Internet of Things Volume G4 Security Framework	7 (<0.01%)	94 (0.031%)	96 (0.26%)	5 (<0.01%)	37 (0.1%)	45 (0.14%)
IoT Trust Framework						1 (0.06%)
Microsoft – Security Best practices for Internet of Things (IoT)		4 (0.07%)				1 (<0.01%)
NIST					4 (0.02%)	
Security Guidance for Early Adopter of the Internet of Things		2 (0.02%)			16 (0.09%)	3 (<0.01%)

The overall word frequency for the organisational factors research objective is visualised in Figure 5.10 and displayed in Table 5.8. The word 'security' is most prevalent. The words following this in prevalence are: 'risk', 'business', 'cost' and 'model'.

Table 5-8: Overall node frequency for Organisational factors

	Organisational				
Document	**Security**	**Risk**	**Business**	**Cost**	**Model**
Industrial Internet of Things Volume G4 Security Framework	42 (0.04%)	35 (0.02%)	15 (<0.01%)	14 (<0.01%)	13 (<0.01%)
IoT Trust Framework					
Microsoft – Security Best practices for Internet of Things (IoT)	3 (<0.01%)				
NIST					
Security Guidance for Early Adopter of the Internet of Things	4 (<0.01%)				
TOTAL	**49**	**35**	**15**	**14**	**13**

Figure 5-10: Overall word frequency for Organisational factors

Next, the work frequency for each organisational factors linked to the research objective is analysed and visualised.

5.4.1 Size and Structure

The word frequency for the factor, ‘size and structure’, is visualised in Figure 5.11. There is no most prevalent word. Since there are no prevalent words and few words, a table of the word frequency for Organisational Factor, size and structure could not be produced. The words are noted: ‘availability’, ‘devices’, ‘group’, ‘individual’, ‘industry’, ‘involve’, ‘large’, ‘multiple’, ‘numbers’, ‘organizations’, ‘posture’, ‘resource’, ‘security’ and ‘physical’. To better understand each of these factors, a text search on the node, ‘size and structure’ under organisational factors, is conducted, and the results are displayed in a word tree for each word.

Figure 5-11: Visualisation of the word frequency for Size and Structure

The text search on the node, ‘size and structure’ under organisational factors, is conducted for each of the words above, and the results of the word trees are displayed in Appendix C (Figure C13 – Figure C. From here, we can see that the factors for the size and structure of IIoT are resource availability.

From the analysis of the frequency of nodes for the factor, ‘size and structure, we can determine that there are no prevalent word and the details of the words are:

- Resource availability.
- The number of devices.
- A group that control or influence.
- An individual that control or influence.
- System’s industry.
- Involving multiple organisations.
- The security posture of the organisation.

Section 6.3.1 discusses the results further, including a unique analysis of the implications for the transport sector.

5.4.2 Cybersecurity Strategy

The word frequency for the factor, ‘Cybersecurity strategy’, is visualised in Figure 5.12 and displayed in Table 5.9. The word ‘security’ is again most prevalent because the cybersecurity strategy focuses on security, and the word security is combined with most of the other words. The words following this in prevalence are: ‘model’, ‘program’, ‘business’, and ‘risk’. To gain a clearer understanding of what ‘security’ strategy and what ‘models’, ‘program’, business’ and ‘risk’ are factors, a text search on the node ‘cybersecurity strategy’ under organisational factors is conducted, and the results displayed in a word tree for each of the most frequent words.

Figure 5-12: Visualisation of the word frequency for Cybersecurity strategy to IIoT

Table 5-9: Table of the word frequency for Cybersecurity strategy to IIoT

	Organisational – Cybersecurity strategy				
Document	**Security**	**Model**	**Program**	**Business**	**Risk**
Industrial Internet of Things Volume G4 Security Framework	31 (0.03%)	9 (<0.01%)	9 (<0.01%)	6 (<0.01%)	6 (<0.01%)
IoT Trust Framework					
Microsoft – Security Best practices for Internet of Things (IoT)	3 (<0.01%)				
NIST					
Security Guidance for Early Adopter of the Internet of Things	2 (<0.01%)				
TOTAL	**36**	**9**	**9**	**6**	**6**

The text search on the node, ‘cybersecurity strategy’ under organisational factors, is conducted for the word ‘security’, and the results of the word tree are displayed in Figure 5.13. From here, we can see the factors for cybersecurity strategy to IIoT are security model, security program/programs, security posture, security objectives, security policies, security in-depth strategy, security controls/countermeasures, security processes, and security risks.

Figure 5-13: Word tree for 'security' under the cybersecurity structure node

The text search on the node, 'cybersecurity strategy' under organisational factors, is conducted for the words 'model', 'program', 'business', and 'risk'. The word tree results are displayed in Appendix C (Figure C26 – C29).

From the analysis of the frequency of nodes for the factor 'cybersecurity strategy', we can conclude that the most prevalent words are:

- **Security:** security model, security program/programs, security posture, security objectives, security policies, security in-depth strategy, security controls/countermeasures, security processes, and security risks.
- **Model**: security model, threat model, Cybersecurity Capability Maturity Model, and model & policy for change management.

- **Program**: security program, program implementation considerations, a program that provides governance, program cost, and the establishment and maintenance of a security program.
- **Business**: business decisions, business needs, business objectives and risk strategy, business priorities, business sectors and verticals.
- **Risk**: managing risk, an organisation's risk appetite, and identifying risk.

Section 6.3.2 discusses the results further, including a unique analysis of the implications for the transport sector.

5.4.3 Risk Appetite

The word frequency for the factor, 'risk appetite', is visualised in Figure 5.14 and displayed in Table 5.10. The word 'risk' is again most prevalent because the word risk is combined with most other words. The words following this in prevalence are: 'cost', 'threat', 'security', and 'business'. To gain a clearer understanding of what the word 'risk' 'cost', 'threat', 'security', and 'business' are factors of, a text search on the node 'risk appetite' under organisational factors are conducted, and the results displayed in a word tree for each of the most frequent words.

Figure 5-14: Visualisation of the word frequency for Organisational Risks to IIoT

Table 5-10: Table of the word frequency for Organisational Risks to IIoT

	Organisational – Risk appetite				
Document	**Risk**	**Cost**	**Threat**	**Security**	**Business**
Industrial Internet of Things Volume G4 Security Framework	30 (<0.01%)	13 (<0.01%)	9 (<0.01%)	8 (<0.01%)	7 (<0.01%)
IoT Trust Framework					

	Organisational – Risk appetite				
Document	**Risk**	**Cost**	**Threat**	**Security**	**Business**
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					
Security Guidance for Early Adopter of the Internet of Things					
TOTAL	**30**	**13**	**9**	**8**	**7**

The text search on the node, 'risk appetite' under organisational factors, is conducted for the word 'risk', and the results of the word tree are displayed in Figure 5.15. From here, we can see the factors for risk appetite to IIoT are risk avoidance, risk strategy, residual risk, outsourcing risk, risk acceptance, risk appetite of an organisation, risk consideration, risk mitigation, risk tolerance, risk transfer, management risk, and risk elimination.

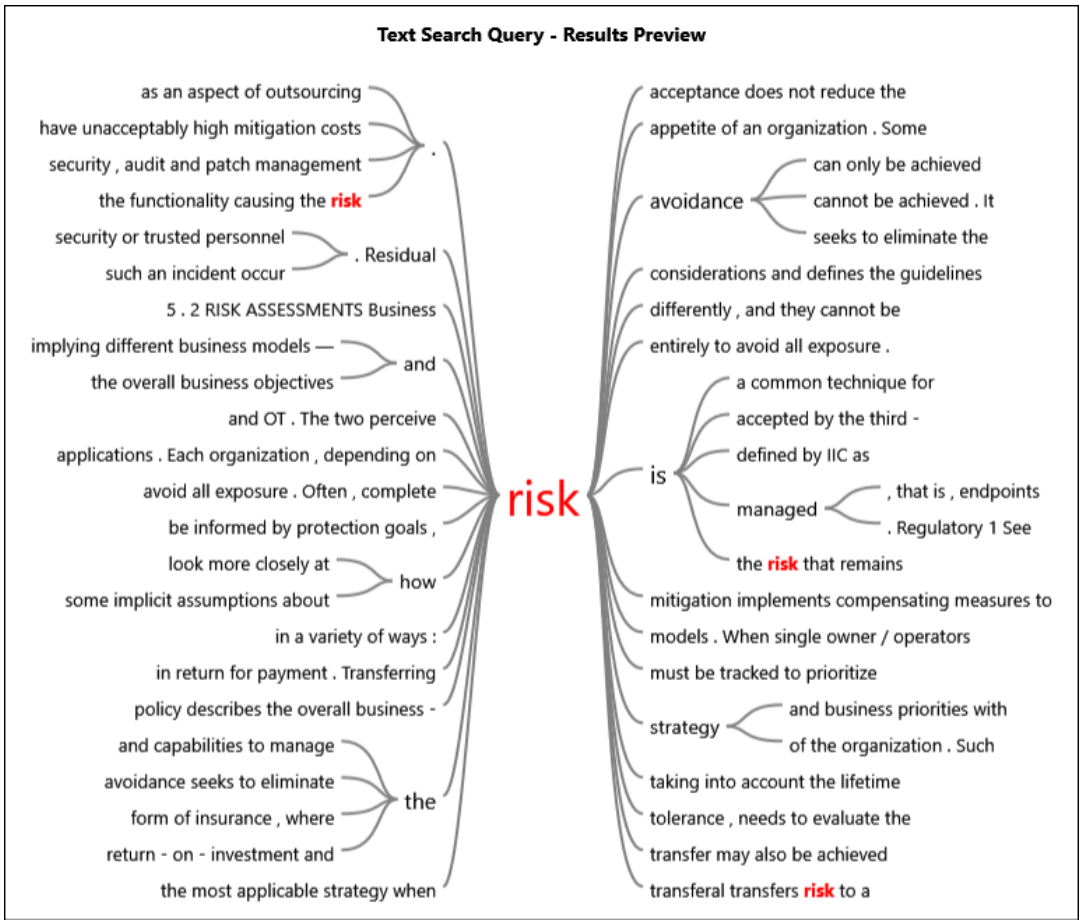


Figure 5-15: Word tree for 'risk' under the risk appetite node

The text search on the node, 'risk appetite' under organisational factors, is conducted for the words cost', 'threat', 'security', and 'business'. The word tree results are displayed in Appendix C (Figure C30 – Figure C33).

From the analysis of the frequency of nodes for the factor ‘risk appetite’, we can conclude that the most prevalent words are:

- **Risk:** risk avoidance, risk strategy, residual risk, outsourcing risk, risk acceptance, risk appetite of an organisation, risk consideration, risk mitigation, risk tolerance, risk transfer, management of risk, and risk elimination.
- **Cost:** replacement cost, cost of an incident/consequence, mitigation exceeds the cost, balance of cost, cost of upgrading security, and cost versus effectiveness of security controls.
- **Threat:** threat model/modelling, threat mitigation, threat actors, threat identification, and impact of unavoidable threat.
- **Security:** cost of upgrading security, cost vs effectiveness of security, security budgets, security controls/countermeasures, security investments, and security risks.
- **Business:** business risk/risks, business objectives, business priorities and business sectors.

Section 6.3.3 discusses the results further, including a unique analysis of the implications for the transport sector.

5.4.4 Innovativeness Culture

The word frequency for the factor, ‘Innovativeness culture’, is visualised in Figure 5.16 and displayed in Table 5.11. The word ‘evolving’ and ‘use’ are most prevalent. For an innovative culture to exist, there needs to be constantly evolving and using people, processes, and technology. The words following this in prevalence are all the same: ‘analytics’, ‘data’, ‘evolution’, ‘expertise’, ‘landscape’, ‘techniques’ and ‘technologies’. To gain a clearer understanding of what ‘evolving’ innovativeness culture and what ‘use’, ‘expertise’, ‘landscape’, ‘techniques’, and ‘technologies’ are factors of, a text search on the node, ‘innovativeness culture’ under organisational factors are conducted and the results displayed in a word tree for each of the most frequent words.

Figure 5-16: Visualisation of the word frequency for Innovativeness culture to IIoT

Table 5-11: Table of the word frequency for Innovativeness culture to IIoT

	Organisational – Innovativeness culture					
Document	**Evolving**	**Use**	**Expertise**	**Landscape**	**Techniques**	**Technologies**
Industrial Internet of Things Volume G4 Security Framework	2 (<0.01%)	2 (<0.01%)	1 (<0.01%)	1 (<0.01%)	1 (<0.01%)	1 (<0.01%)
IoT Trust Framework						
Microsoft – Security Best practices for Internet of Things (IoT)						
NIST						
Security Guidance for Early Adopter of the Internet of Things						
TOTAL	**2**	**2**	**1**	**1**	**1**	**1**

The text search on the node, 'Innovativeness culture' under organisational factors, is conducted for the word 'evolving', and the results of the word tree are displayed in Figure 5.17. From here, we can see the factors for innovativeness culture to IIoT are evolving data analytics techniques and evolving landscape of endpoint and communication.

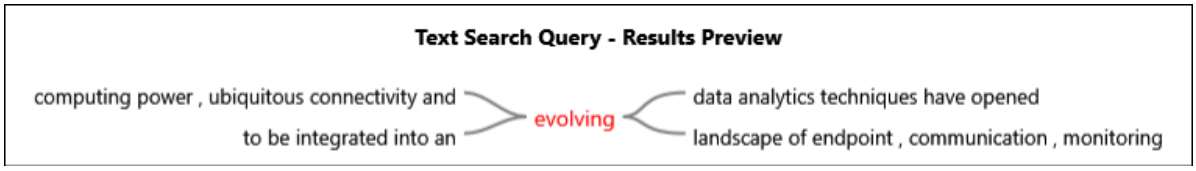


Figure 5-17: Word tree for 'evolving' under the innovativeness culture node

The text search on the node, 'Innovativeness culture' under organisational factors, is conducted for the word 'use', and the results of the word tree are displayed in Figure 5.18. From here, we can see the factors for innovativeness culture to IIoT are the use of technologies and expertise.

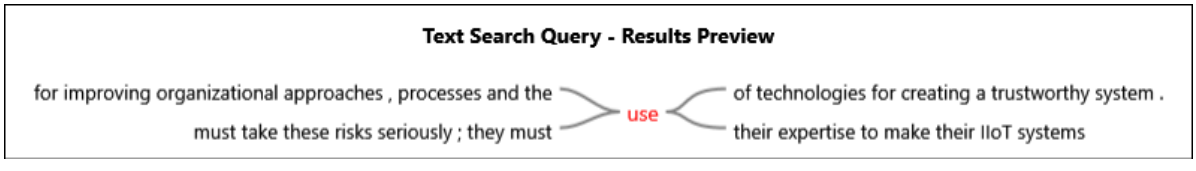


Figure 5-18: Word tree for 'use' under the innovativeness culture node

The text search on the node, 'Innovativeness culture' under organisational factors, is conducted for each of the non-prevalent words, 'analytics', 'data', 'evolution', 'expertise', 'landscape', 'techniques' and 'technologies'. The word tree results are displayed in Appendix C (Figure C34 – Figure C40).

From the analysis of the frequency of nodes for the factor, ‘innovativeness culture’, we can conclude that the most prevalent words are:

- Evolving data analytics techniques.
- Evolving landscape of endpoint and communication.
- Use of technologies and use of expertise.
- Evolution in both business and implementation.
- Use expertise to make their IIoT systems trustworthy.
- Evolving data analytics techniques.
- Technologies for creating a trustworthy system.

Section 6.3.4 discusses the results further, including a unique analysis of the implications for the transport sector.

5.4.5 Security Culture

The word frequency for the factor, ‘security culture’, is visualised in Figure 5.19 and displayed in Table 5.12. The words ‘awareness’ and ‘security’ are the most prevalent. This is because awareness is a crucial driver to ensuring a security culture is embedded in an organisation and security are combined with most other words. The words following this in prevalence are: ‘different’, ‘convergence’, ‘situational’, ‘train’, and ‘understand’. To gain a clearer understanding of what ‘awareness’, ‘security’, ‘different’, ‘situational’, ‘train’, and ‘convergence’ are factors of, a text search on the node, ‘Security culture’ under organisational factors is conducted, and the results displayed in a word tree for each of the most frequent words.

Figure 5-19: Visualisation of the word frequency for Security culture to IIoT

Table 5-12: Table of the word frequency for Security culture to IIoT

	Organisational – Security culture						
Document	**Awareness**	**Security**	**Different**	**Convergence**	**Situational**	**Train**	**Understand**
Industrial Internet of Things Volume G4 Security Framework	1 (<0.01%)	5 (<0.01%)	5 (<0.01%)	3 (<0.01%)			1 (<0.01%)
IoT Trust Framework							
Microsoft – Security Best practices for Internet of Things (IoT)							
NIST	1 (<0.01%)						2 (<0.01%)
Security Guidance for Early Adopter of the Internet of Things	5 (<0.01%)	2 (<0.01%)			3 (<0.01%)	3 (<0.01%)	
TOTAL	**7**	**7**	**5**	**3**	**3**	**3**	**3**

The text search on the node, 'security culture' under organisational factors, is conducted for the word' awareness', and the results of the word tree are displayed in Figure 5.20. From here, we can see the factors for security culture to IIoT are security-aware culture, instil awareness, situational awareness, adequate awareness and awareness accountability and responsibility.

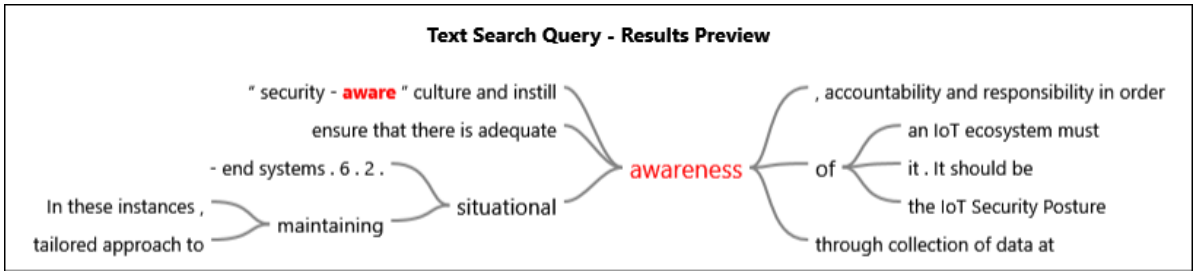


Figure 5-20: Word tree for 'awareness' under the security culture node

The text search on the node, 'security culture' under organisational factors, is conducted for the word 'security', and the results of the word tree are displayed in Figure 5.21. From here, we can see the factors for security culture to IIoT are developing a security-aware culture, security evangelists, difficulty applying security, the organisation's security posture, and security being overlooked or less critical in OT.

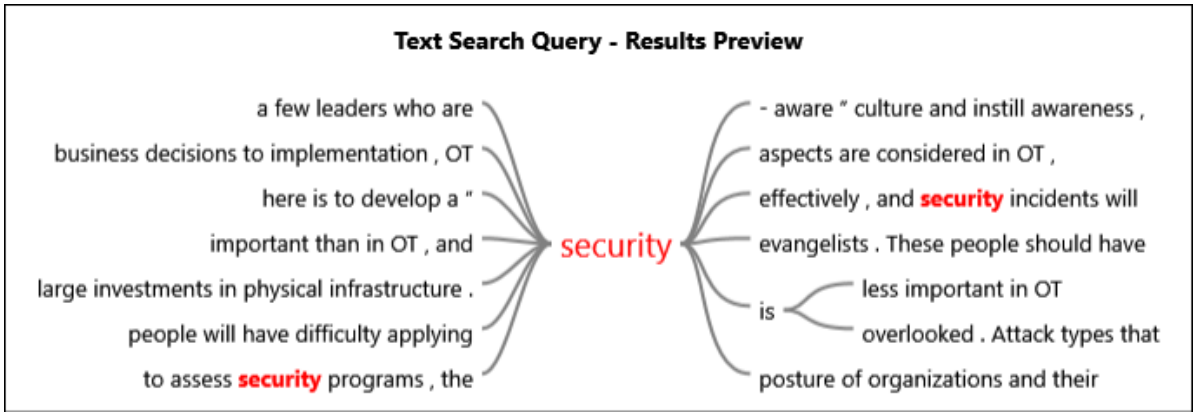


Figure 5-21: Word tree for 'security' under the security culture node

The text search on the node, 'security culture' under organisational factors, is conducted for the words 'different', 'convergence', 'situational', 'train', and 'understand'. The word tree results are displayed in Appendix C (Figure C41 – Figure C45).

From the analysis of the frequency of nodes for the factor' security culture', we can conclude that the most prevalent words are:

- **Awareness**: security-aware culture, instil awareness, situational awareness, adequate awareness and awareness accountability and responsibility.
- **Security**: security-aware culture, instil awareness, situational awareness, adequate awareness and awareness accountability and responsibility.
- **Different**: security-aware culture, instil awareness, situational awareness, adequate awareness and awareness accountability and responsibility.
- **Convergence**: security-aware culture, instil awareness, situational awareness, adequate awareness and awareness accountability and responsibility.
- **Situational**: security-aware culture, instil awareness, situational awareness, adequate awareness and awareness accountability and responsibility.
- **Train**: constantly train, train end users, and train staff.
- **Understand**: understand characteristics of IoT affect managing cybersecurity and understand use of IoT.

Section 6.3.5 discusses the results further, including a unique analysis of the implications for the transport sector.

5.4.6 Senior Executive Engagement with Security

The word frequency for the factor, 'Senior executive engagement with security', is visualised in Figure 5.22 and displayed in Table 5.13. The word 'communicated' is again the most prevalent. Without communication, engagement is not possible. The words following this in prevalence are: 'decision', 'security', 'stakeholders', and 'business'. To gain a clearer understanding of what 'communicated',

'decision', 'security', 'stakeholders', and 'business' are factors of, a text search on the node, 'Senior executive engagement with security' under organisational factors are conducted, and the results displayed in a word tree for each of the most frequent words.

Figure 5-22: Visualisation of the word frequency for senior executive engagement with security to IIoT

Table 5-13: Table of the word frequency for senior executive engagement with security to IIoT

	Organisational – Senior executive engagement with security				
Document	**Communicated**	**Decision**	**Security**	**Stakeholders**	**Business**
Industrial Internet of Things Volume G4 Security Framework	7 (<0.01%)	7 (<0.01%)	5 (<0.01%)	6 (<0.01%)	5 (<0.01%)
IoT Trust Framework	1 (<0.03%)				
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					
Security Guidance for Early Adopter of the Internet of Things			1 (<0.01%)		
TOTAL	**8**	**7**	**6**	**6**	**5**

The text search on the node, 'senior executive engagement with security' under organisational factors, is conducted for the word 'communicated', and the results of the word tree are displayed in Figure 5.23. From here, we can see that the factors for senior executive engagement with security to IIoT are communicated effectively and communicated to business decision-makers.

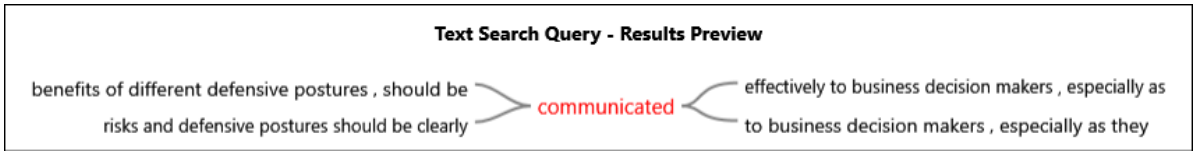


Figure 5-23: Word tree for 'communicated' under the senior executive engagement node

The text search on the node, 'Senior executive engagement with security' under organisational factors, is conducted for the words 'decision', 'security', 'stakeholders', and 'business'. The word tree results are displayed in Appendix C (Figure C46 – Figure C49).

From the analysis of the frequency of nodes for the factor, 'senior executive engagement with security, we can conclude that the most prevalent words are:

- **Communicated**: communicated effectively and communicated to business decision-makers.
- **Decision**: effective business decision, decision makers and decision making.
- **Security**: security metrics, security effectiveness, security evangelists, security programs, security risks, accurate representation of security, and increased accountability to improve security.
- **Stakeholders**: stakeholders expect/expectations include all stakeholders, prioritised by stakeholders, justified to stakeholders, and stakeholders by reference to the business risks.
- **Business**: business decision makers/making, communicated to business, and business decisions.

Section 6.3.6 discusses the results further, including a unique analysis of the implications for the transport sector.

5.5 Procedural Factors Influencing IIoT Cybersecurity

The next section evaluates the procedural factors influencing IIoT cybersecurity. To determine the extent to which the procedural factors influence IIoT cybersecurity, nodes are created to link the references to procedural factors in the five (5) documents analysed via NVivo. Table 5.14 summarise the count and percentage (%) of nodes for each of the procedural factors (Security incident response, Risk management, IT governance and compliance, Policies, standards, and procedures, Legal and regulatory requirements) per document analysed. From here we can see majority of the nodes coded under procedural factors are from the document 'Industrial Internet of Things Volume G4 Security Framework'.

Table 5-14: Summary of Procedural factors

	Procedural				
Document	**Security incident response**	**Risk management**	**IT governance and compliance**	**Policies, standards, and procedures**	**Legal and regulatory requirements**
Industrial Internet of Things Volume G4 Security Framework	118 (0.32%)	156 (0.57%)	24 (0.06%)	199 (0.59%)	30 (0.08%)
IoT Trust Framework	5 (0.24%)	2 (0.21%)		16 (0.77%)	3 (0.33%)
Microsoft – Security Best practices for Internet of Things (IoT)		10 (0.08%)		6 (0.08%)	
NIST		2 (0.05%)		3 (0.04%)	
Security Guidance for Early Adopter of the Internet of Things	8 (0.07%)	15 (0.11%)		100 (0.98%)	2 (0.02%)
TOTAL	**131**	**185**	**24**	**324**	**35**

The overall word frequency for the procedural factors research objective is visualised in Figure 5.24 and displayed in Table 5.15. The word ‘security’ is most prevalent. The words following this in prevalence are: ‘policy’, ‘risk’, ‘threat’, and ‘data’.

Table 5-15: Overall node frequency for Procedural factors

	Procedural				
Document	**Security**	**Policy**	**Risk**	**Threat**	**Data**
Industrial Internet of Things Volume G4 Security Framework	76 (0.07%)	53 (0.04%)	39 (0.02%)	14 (<0.01%)	12 (<0.01%)
IoT Trust Framework	4 (0.08%)	5 (0.08%)	1 (0.01%)		2 (0.02%)
Microsoft – Security Best practices for Internet of Things (IoT)	1 (<0.01%)	3 (<0.01%)		8 (0.03%)	
NIST		1 (<0.01%)	2 (<0.01%)		
Security Guidance for Early Adopter of the Internet of Things	20 (0.05%)	13 (0.03%)	2 (<0.01%)	5 (<0.01%)	10 (<0.01%)
TOTAL	**101**	**75**	**44**	**27**	**24**

Figure 5-24: Overall word frequency for Procedural factors

Next, the work frequency for each procedural factors linked to the research objective is analysed and visualised.

5.5.1 Security Incident Response

The word frequency for the factor, ‘Security incident response’, is visualised in Figure 5.25 and displayed in Table 5.16. The word ‘monitoring’ is again most prevalent. Monitoring is crucial in incident response. Without monitoring, detecting incidents would not be possible, and a response would be too late. The words following this in prevalence are: ‘response’, ‘analysis’, ‘plan’, and ‘security’. To gain a clearer understanding of what ‘monitoring’ response’, ‘analysis’, ‘plan’, and ‘security’ are factors of a text search on the node, ‘Security incident response’ under procedural factors are conducted, and the results displayed in a word tree for each of the most frequent words.

Figure 5-25: Visualisation of the word frequency for Security incident response to IIoT

Table 5-16: Table of the word frequency for Security incident response to IIoT

	Procedural – Security incident response				
Document	**Monitoring**	**Response**	**Analysis**	**Security**	**Incident**
Industrial Internet of Things Volume G4 Security Framework	16 (0.02%)	13 (<0.01%)	11 (<0.01%)	10 (<0.01%)	8 (<0.01%)
IoT Trust Framework		1 (0.02%)			
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					
Security Guidance for Early Adopter of the Internet of Things		1 (<0.01%)			1 (<0.01%)
TOTAL	**16**	**15**	**11**	**10**	**9**

The text search on the node, ‘Security incident response’ under procedure factors, is conducted for the word ‘monitoring’, and the results of the word tree are displayed in Figure 5.26. From here, we can see the factors for Security incident response to IIoT are monitoring and analysis, monitoring encrypted channels, monitoring captures, monitoring of data, and monitoring tools.

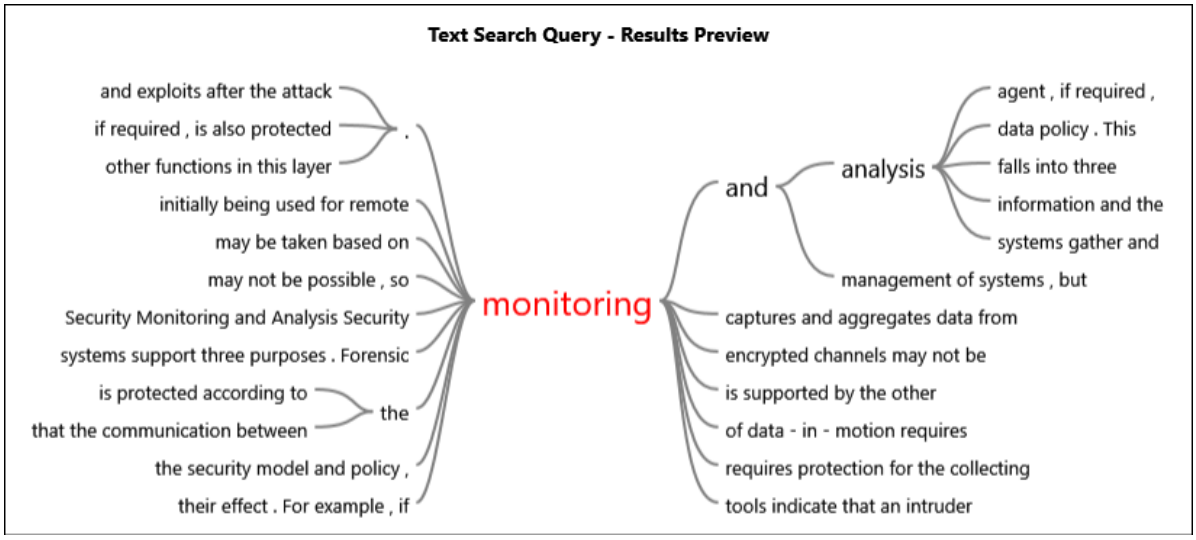


Figure 5-26: Word tree for 'monitoring' under security incident response node

The text search on the node, 'Security incident response' under procedure factors, is conducted for the words 'response', 'analysis', 'plan', and 'security'. The word tree results are displayed in Appendix C (Figure C50 – Figure C53).

From the analysis of the frequency of nodes for the factor, 'Security incident response', we can conclude that the most prevalent words are:

- **Monitoring**: monitoring and analysis, monitoring encrypted channels, monitoring captures, monitoring of data, and monitoring tools.
- **Response**: incident response plan/plans, rapid response, and response and consumer notification plan.
- **Analysis**: monitoring and analysis, rule-based analysis, forensic analysis, root cause analysis, behavioural analysis, analysis agent, analysis data policy, analysis monitors for violations, analysis observes usage patterns, analysis of previous attacks, and analysis uses looks for events.
- **Security**: identify and detect security, security control configurations, security issues, violation of security, security model and policy, security monitoring, security responses, security thresholds, and security violations.
- **Incident**: incident response plan/plans, incident investigations and root cause analysis, incident model, and automated incident response.

Section 6.4.1 discusses the results further, including a unique analysis of the implications for the transport sector.

5.5.2 Risk Management

The word frequency for the factor, 'Risk management', is visualised in Figure 5.27 and displayed in Table 5.17. The word 'risk' is again most prevalent. This is because the word risk is combined with most other words. The words following this in prevalence are: 'threat', 'modelling', 'security', and 'assessment'. To gain a clearer understanding of what 'risk', threat', 'modelling', 'security', and 'assessment' are the factors of a text search on the node, 'Risk management' under procedural factors is conducted, and the results displayed in a word tree for each of the most frequent words.

Figure 5-27: Visualisation of the word frequency for Risk management to IIoT

Table 5-17: Table of the word frequency for Risk management to IIoT

	Procedural – Risk Management				
Document	**Risk**	**Threat**	**Modelling**	**Security**	**Cost**
Industrial Internet of Things Volume G4 Security Framework	38 (0.02%)	11 (<0.01%)	4 (<0.01%)	14 (<0.01%)	13 (<0.01%)
IoT Trust Framework	1 (<0.01%)			1 (0.02%)	
Microsoft – Security Best practices for Internet of Things (IoT)		8 (0.03%)	8 (0.04%)		
NIST	2 (<0.01%)				
Security Guidance for Early Adopter of the Internet of Things	2 (<0.01%)	5 (<0.01%)	4 (<0.01%)	1 (<0.01%)	
TOTAL	**43**	**24**	**16**	**16**	**13**

The text search on the node, ‘Risk management’ under procedure factors, is conducted for the word ‘risk’, and the results of the word tree are displayed in Figure 5.28. From here, we can see the factors for Risk management to IIoT are risk assessment/assessments, risk avoidance, risk analysis, risk strategy, transferring risk, residual risk, quantitative risk, risk considerations, risk mitigation, risk models and risk acceptance.

Figure 5-28: Word tree for ‘risk’ under risk management node

The text search on the node, ‘Risk management’ under procedure factors, is conducted for the words ‘threat’, ‘modelling’, ‘security’, and ‘assessment’. The word tree results are displayed in Appendix C (Figure C54 – Figure C57).

From the analysis of the frequency of nodes for the factor ‘Risk management, we can conclude that the most prevalent words are:

- **Risk**: risk assessment/assessments, risk avoidance, risk analysis, risk strategy, transferring risk, residual risk, quantitative risk, risk considerations, risk mitigation, risk models and risk acceptance.
- **Threat**: threat modelling, threat analysis, threat mitigation, threat identification, and threat intelligence.
- **Modelling**: threat modelling.
- **Security**: security risks, security concerns, security audit, security controls & countermeasures, security issues, security models, prioritise security, security programs, and improve security.
- **Cost**: cost of compromise, cost of consequences/incidents, cost versus effectiveness of security controls, mitigation exceeds the cost, and cost of upgrading security systems.

Section 6.4.2 discusses the results further, including a unique analysis of the implications for the transport sector.

5.5.3 IT Governance and Compliance

The word frequency for the factor, ‘IT governance and compliance’, is visualised in Figure 5.29 and displayed in Table 5.18. The words ‘compliance’ and ‘security’ are most prevalent. This is because the word compliance is combined with most other words. The words following this in prevalence are: ‘management’, ‘governance’, and ‘assurance’. To gain a clearer understanding of what ‘compliance’, ‘security’, ‘management’, ‘governance’, and ‘assurance’ are factors of a text search on the node, ‘IT governance and compliance’ under procedural factors are conducted and the results displayed in a word tree for each of the most frequent words.

Figure 5-29: Visualisation of the word frequency for IT Governance and compliance to IIoT

Table 5-18: Table of the word frequency for IT Governance and compliance to IIoT

	Procedural – IT Governance and compliance				
Document	**Compliance**	**Security**	**Assurance**	**Governance**	**Management**
Industrial Internet of Things Volume G4 Security Framework	4 (<0.01%)	4 (<0.01%)	3 (<0.01%)	3 (<0.01%)	3 (<0.01%)
IoT Trust Framework					
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					
Security Guidance for Early Adopter of the Internet of Things					
TOTAL	**4**	**4**	**3**	**3**	**3**

The text search on the node, 'IT Governance and compliance' under procedure factors, are conducted for the word 'compliance', and the results of the word tree are displayed in Figure 5.30. From here, we can see the factors for IT Governance and compliance to IIoT are regulatory and compliance, compliance requirements and required compliance.

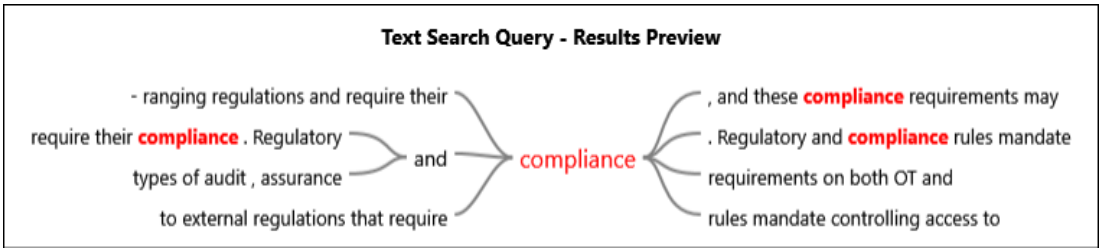


Figure 5-30: Word tree for 'compliance' under IT governance and compliance node

The text search on the node, 'IT Governance and compliance' under procedure factors, are conducted for the word 'security', and the results of the word tree are displayed in Figure 5.31. From here, we can see the factors for IT Governance and compliance to IIoT are Processes that governance security, implementation of security, assurance of security, security configuration management, security functions, security assessment, and security policies.

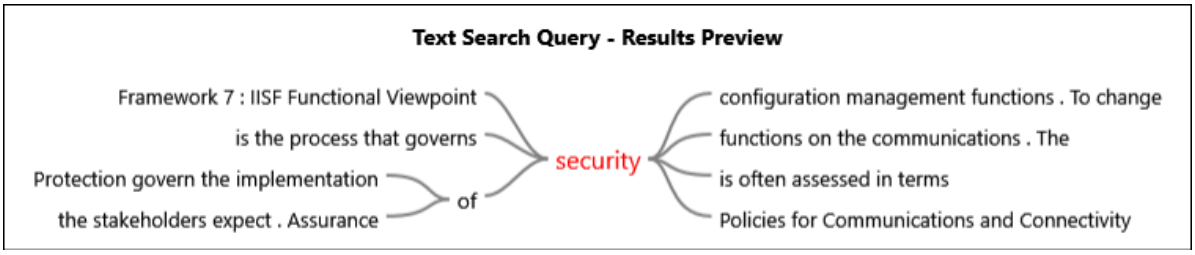


Figure 5-31: Word tree for 'security' under IT governance and compliance node

The text search on the node, 'IT Governance and compliance' under procedure factors, is conducted for the words 'management', 'governance', and 'assurance'. The word tree results are displayed in Appendix C (Figure C58 – Figure C60).

From the analysis of the frequency of nodes for the factor, 'IT Governance and compliance, we can conclude that the most prevalent words are:

- **Compliance**: regulatory compliance, compliance requirements, and required compliance.
- **Security**: Process that governance security, implementation of security, assurance of security, security configuration management, security functions, security assessed, and security policies.
- **Assurance**: assurance and compliance requirements, assurance of security, types of audit assurance, and assurance of key system characteristics.
- **Governance**: security program that provides governance, efficient management and governance, and key performance indicators.
- **Management**: efficient management, governs security configuration management, management and governance, management functions, and management of systems.

Section 6.4.3 discusses the results further, including a unique analysis of the implications for the transport sector.

5.5.4 Policies, Standards and Procedures,

The word frequency for the factor, 'Policies, standards, and procedures', is visualised in Figure 5.32 and displayed in Table 5.19. The word 'security' is again most prevalent. Security is the focus of each policy, standard and procedure, hence the most prevalent. The words following this in prevalence are: 'policy', 'framework', 'processes', and 'data'. To gain a clearer understanding of what 'security', 'policy', 'framework', 'processes', and 'data' are factors of, a text search on the node, 'Policies, procedures, standards, and frameworks' under procedural factors are conducted and the results displayed in a word tree for each of the most frequent words.

Figure 5-32: Visualisation of the word frequency for Policies, standards, and procedures to IIoT

Table 5-19: Table of the word frequency for Policies, standards, and procedures to IIoT

	Procedural – Policies, standards, and procedures				
Document	**Security**	**Policy**	**Data**	**Communication**	**Framework**
Industrial Internet of Things Volume G4 Security Framework	52 (0.05%)	45 (0.04%)	10 (<0.01%)	16 (0.03%)	5 (<0.01%)
IoT Trust Framework	2 (0.04%)	5 (0.08%)	1 (<0.01%)	1 (0.03%)	
Microsoft – Security Best practices for Internet of Things (IoT)	1 (<0.01%)	3 (<0.01%)			
NIST		1 (<0.01%)			
Security Guidance for Early Adopter	19 (0.05%)	13 (0.03%)	10 (<0.01%)		11 (0.04%)

	Procedural – Policies, standards, and procedures				
Document	**Security**	**Policy**	**Data**	**Communication**	**Framework**
of the Internet of Things					
TOTAL	**74**	**67**	**21**	**17**	**16**

The text search on the node, ‘Policies, standards, and procedures’ under procedure factors, is conducted for the word ‘security’, and the results of the word tree are displayed in Figure 5.33. From here, we can see the factors for Policies, standards, and procedures to IIoT are security policy/policies, security model, security objectives, security controls, security framework, security data, and security events.

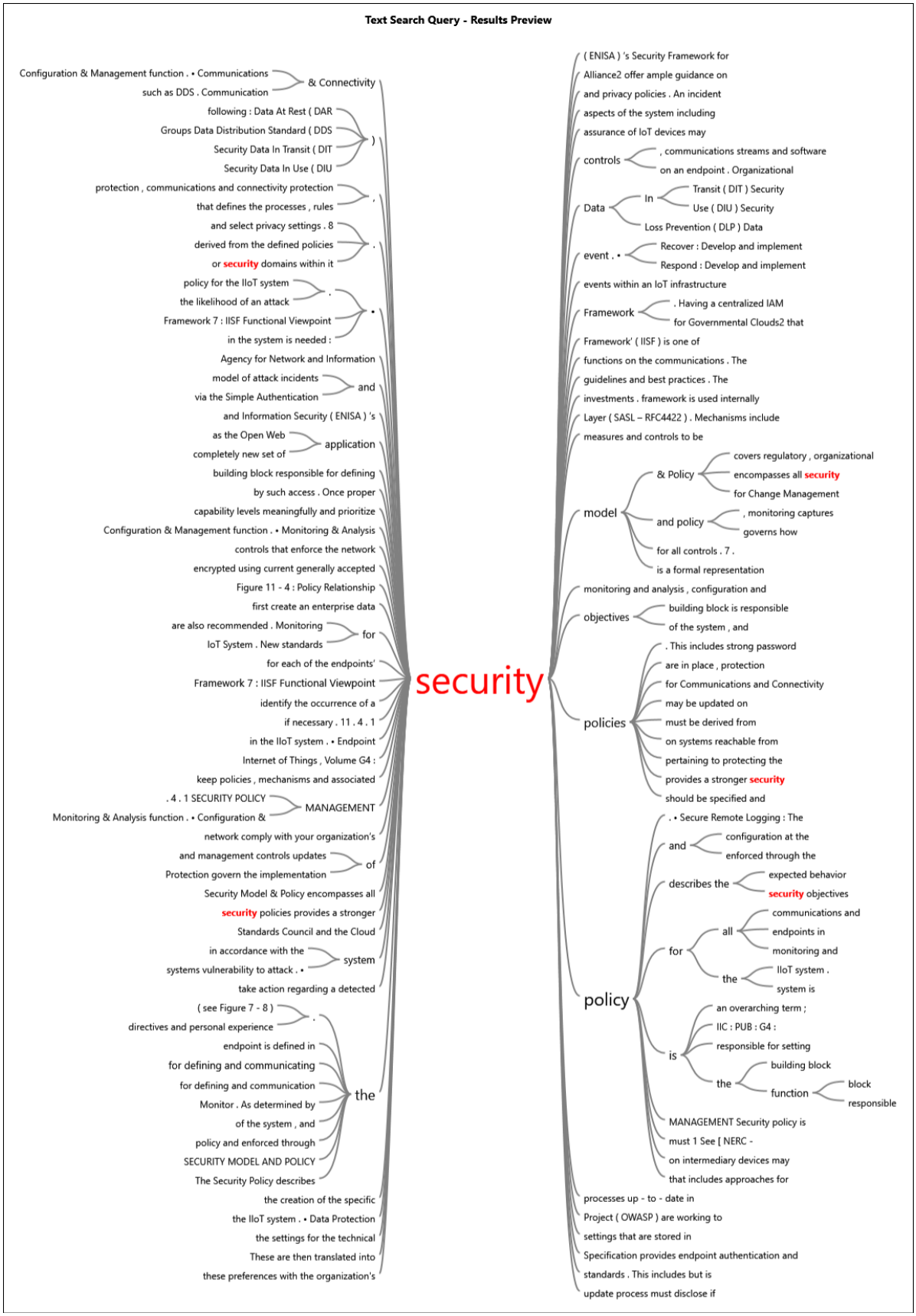


Figure 5-33: Word tree for 'security' under policies, standards, and procedures node

The text search on the node, ‘Policies, standards, and procedures’ under procedure factors, is conducted for the words ‘policy’, ‘framework’, ‘processes’, and ‘data’. The word tree results are displayed in Appendix C (Figure C61 – Figure C64).

From the analysis of the frequency of nodes for the factor, ‘Policies, standards, and procedures’, we can conclude that the most prevalent words are:

- **Security**: security policy/policies, security model, security objectives, security controls, security framework, security data, and security events.
- **Policy**: security policy, security model and policy, and various policies (data retention policy, password policy, organisational policy, data protection policy, endpoint protection).
- **Data**: security data, data protection, data breach, data retention, data loss prevention (DLP), data integrity, personal data, data policy, and monitoring and analysis of data.
- **Communications**: communication and connectivity, communication processes, communication streams, and security policies for communication.
- **Framework**: security framework, logging/audit framework, authentication/authorisation framework, defining a framework for the organisation’s IoT deployment/ecosystem, ENISA’s and NIST framework, a framework for secure development, and framework for secure coding practices.

Section 6.4.4 discusses the results further, including a unique analysis of the implications for the transport sector.

5.5.5 Legal and Regulatory Requirements

The word frequency for the factor, ‘Legal and regulatory requirements’, is visualised in Figure 5.34 and displayed in Table 5.20. The word ‘regulations’ is again most prevalent. This is because the word regulations are combined with most other words. The words following this in prevalence are: ‘regulatory’, ‘privacy’, ‘policy’, and ‘compliance’. To gain a clearer understanding of what ‘regulations’, ‘regulatory’, ‘privacy’, ‘policy’, and ‘compliance’ are the factors of a text search on the node, ‘Legal and regulatory requirements under procedural factors are conducted and the results displayed in a word tree for each of the most frequent words.

Figure 5-34: Visualisation of the word frequency for Legal and regulatory requirements to IIoT

Table 5-20: Visualisation of the word frequency for Legal and regulatory requirements to IIoT

	Procedural – Legal and regulatory requirements				
Document	**Regulations**	**Regulatory**	**Policy**	**Privacy**	**Compliance**
Industrial Internet of Things Volume G4 Security Framework	10 (<0.01%)	6 (<0.01%)	4 (<0.01%)	2 (<0.01%)	3 (<0.01%)
IoT Trust Framework		1 (0.02%)		2 (0.03%)	
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					
Security Guidance for Early Adopter of the Internet of Things	1 (0.03%)				
TOTAL	**11**	**7**	**4**	**4**	**3**

The text search on the node, ‘Legal and regulatory requirements’ under procedure factors, is conducted for the word ‘Regulations’, and the results of the word tree are displayed in Figure 5.35. From here, we can see the factors for Legal and regulatory requirements to IIoT are privacy regulations, security regulations, IT and OT regulations, staying up to date with regulations, external regulations, compliance with regulations, safety regulations, regulations are of increasing importance, and ranging regulations.

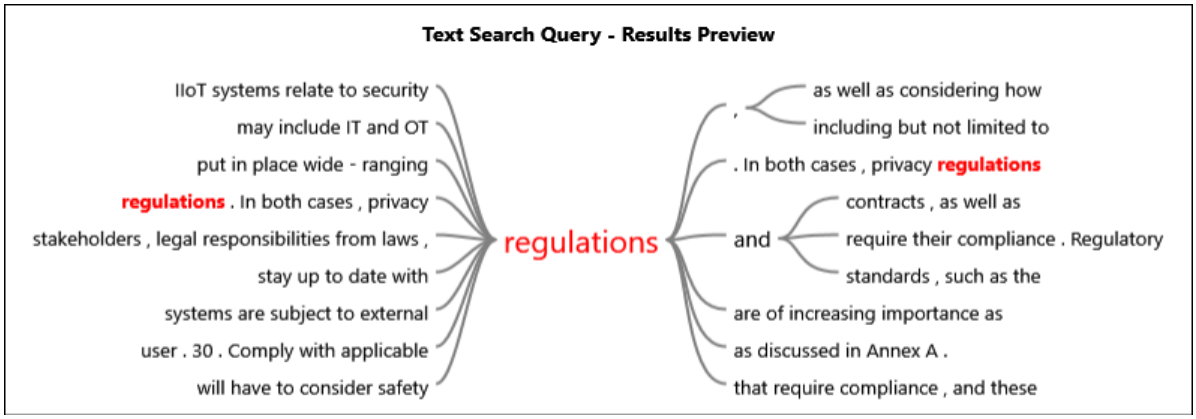


Figure 5-35: Word tree for 'regulations' under legal and regulatory requirements node

The text search on the node, 'Legal and regulatory requirements' under procedure factors, is conducted for the words 'regulatory', 'privacy', 'policy', and 'compliance'. The word tree results are displayed in Appendix C (Figure C65 -Figure C68).

From the analysis of the frequency of nodes for the factor 'Legal and regulatory requirements, we can conclude that the most prevalent words are:

- **Regulations**: privacy regulations, security regulations, IT and OT regulations, staying up to date with regulations, external regulations, compliance with regulations, safety regulations, and regulations are of increasing importance, and ranging regulations.
- **Regulatory**: regulatory policy, regulatory requirements, regulatory and compliance rules, security, and data transfer regulations and match the directives from the regulatory.
- **Policy**: regulatory policy, changes to regulatory policy, directives from regulatory policy, regulatory policy strengthen network access controls, and policy to industry standards.
- **Privacy**: International privacy, privacy protection act, privacy regulations, privacy, security, and data transfer regulations.
- **Compliance**: require compliance, regulatory compliance, compliance business process, and compliance rules mandate.

Section 6.4.5 discusses the results further, including a unique analysis of the implications for the transport sector.

5.6 People Factors Influencing IIoT Cybersecurity

The following section evaluates the people factors influencing IIoT cybersecurity. To determine the extent to which the people factors influence IIoT cybersecurity, nodes are created to link the references to people factors in the five documents analysed via NVivo. Table 5.21 summarises the count and percentage (%) of nodes for each of the people factors (Cybersecurity awareness, enablement, employee engagement, and employee satisfaction) per document analysed. From here, we can see

most of the nodes coded under people factors are from the document ‘Security Guidance for Early Adopter of the Internet of Things’.

Table 5-21: Summary of People factors

	People			
Document	**Cybersecurity awareness**	**Enablement**	**Employee engagement**	**Employee satisfaction**
Industrial Internet of Things Volume G4 Security Framework		9 (0.02%)	1 (<0.01%)	1 (<0.01%)
IoT Trust Framework	3 (0.13%)	4 (0.31%)	7 (0.38%)	3 (0.06%)
Microsoft – Security Best practices for Internet of Things (IoT)				
NIST			1 (<0.01%)	1 (<0.01%)
Security Guidance for Early Adopter of the Internet of Things	20 (0.12%)	10 (0.05%)	5 (0.07%)	2 (<0.01%)
TOTAL	**23**	**23**	**14**	**7**

The overall word frequency for the people factors research objective is visualised in Figure 5.36 and displayed in Table 5.22. The word ‘awareness’ is most prevalent. The words following this in prevalence are: ‘train’, ‘situational’, ‘user’, and ‘consumer’.

Table 5-22: Overall node frequency for People factors

	People				
Document	**Awareness**	**Train**	**Situational**	**User**	**Consumer**
Industrial Internet of Things Volume G4 Security Framework		1 (<0.01%)			
IoT Trust Framework	1 (<0.01%)			2 (0.02%)	4 (0.08%)
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					
Security Guidance for Early Adopter of the Internet of Things	9 (<0.01%)	5 (<0.01%)	5 (0.02%)	2 (<0.01%)	
TOTAL	**10**	**6**	**5**	**4**	**4**

Figure 5-36: Overall word frequency for People factors

Next, the work frequency for each people factors linked to the research objective is analysed and visualised.

5.6.1 Cybersecurity Awareness

The word frequency for the factor, ‘Cybersecurity awareness’, is visualised in Figure 5.37 and displayed in Table 5.23. The word ‘awareness’ is most prevalent. This is because the word awareness is combined with most other words. The words following this in prevalence are: ‘situational’, ‘train’, ‘user’, and ‘made’. To gain a clearer understanding of what ‘awareness’ ‘situational’, ‘train’, ‘user’, and ‘made’ factors of, a text search on the node, ‘Cybersecurity awareness’ under people factors is conducted, and the results displayed in a word tree for each of the most frequent words.

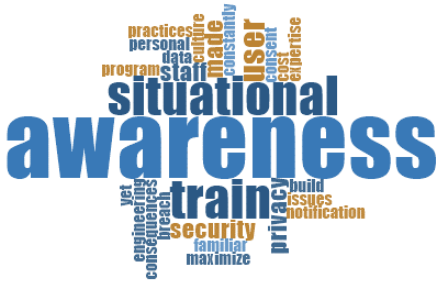


Figure 5-37: Visualisation of the word frequency for Cybersecurity awareness to IIoT

Table 5-23: Visualisation of the word frequency for Legal and regulatory requirements to IIoT

	People – Cybersecurity awareness				
Document	**Awareness**	**Situational**	**Train**	**User**	**Made**
Industrial Internet of Things Volume G4 Security Framework					
IoT Trust Framework	1 (<0.01%)			1 (<0.01%)	
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					
Security Guidance for Early Adopter of the Internet of Things	9 (0.02%)	5 (<0.01%)	5 (<0.01%)	2 (<0.01%)	2 (<0.01%)
TOTAL	**10**	**5**	**5**	**3**	**2**

The text search on the node, 'cybersecurity awareness' under people factors, is conducted for the word 'awareness', and the results of the word tree are displayed in Figure 5.38. From here, we can see the factors for cybersecurity awareness of IIoT are situational awareness, security-aware culture, maximising user awareness, awareness of IoT security, and awareness through a collection of data.

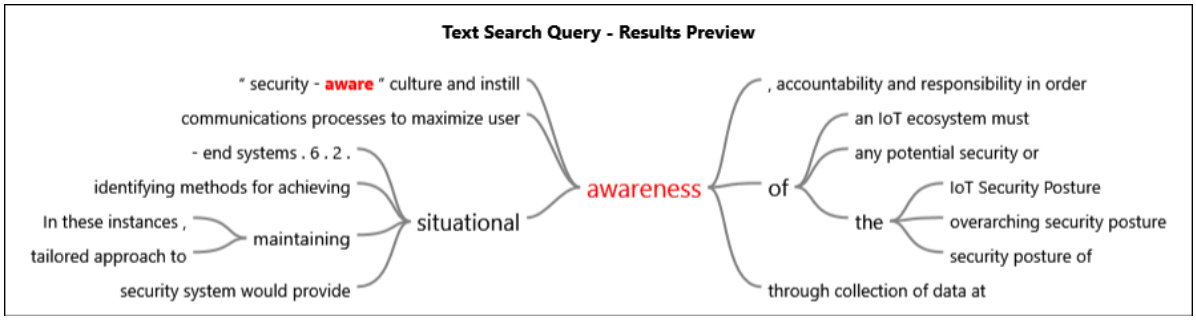


Figure 5-38: Word tree for 'awareness' under cybersecurity awareness node

The text search on the node, 'cybersecurity awareness' under people factors, is conducted for the words 'situational', 'train', 'user', and 'made'. The word tree results are displayed in Appendix C (Figure C69 - Figure C72).

From the analysis of the frequency of nodes for the factor 'cybersecurity awareness, we can conclude that the most prevalent words are:

- **Awareness**: situational awareness, security-aware culture, maximise user awareness, awareness of IoT security, and awareness through data collection.

- **Situational**: situational awareness, maintaining and achieving situational awareness.
- **Train**: train staff, train users, constantly train, and cost to train.
- **User**: communications processes to maximise user awareness and user consent.
- **Made**: Stakeholders should be made aware, and IoT systems should be made aware.

Section 6.5.1 discusses the results further, including a unique analysis of the implications for the transport sector.

5.6.2 Enablement

The word frequency for the factor, 'Enablement', is visualised in Figure 5.39 and displayed in Table 5.24. The word 'train' is again most prevalent. Training is critical to enable staff, and the focus should be on training and upskilling staff. The words following this in prevalence are: 'human', 'identifiable', 'expertise', and 'staff'. To gain a clearer understanding of what 'train' human', 'identifiable', 'expertise', and 'staff' are the factors of, a text search on the node 'enablement' under people factors is conducted, and the results displayed in a word tree for each of the most frequent words.

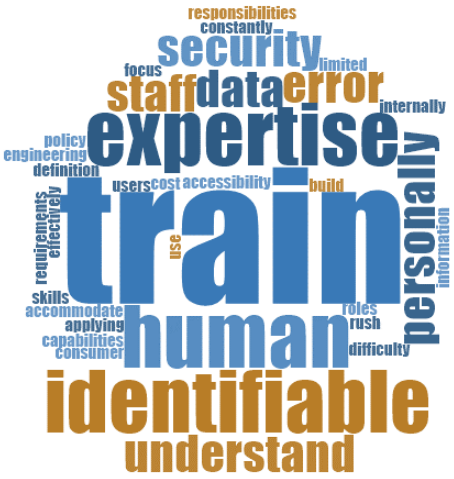


Figure 5-39: Visualisation of the word frequency for Enablement to IIoT

Table 5-24: Table of the word frequency for Enablement to IIoT

	People – Enablement				
Document	**Train**	**Expertise**	**Human**	**Identifiable**	**Staff**
Industrial Internet of Things Volume G4 Security Framework	1 (<0.01%)	1 (<0.01%)	3 (<0.01%)		
IoT Trust Framework				3 (0.09%)	
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					

	People – Enablement				
Document	**Train**	**Expertise**	**Human**	**Identifiable**	**Staff**
Security Guidance for Early Adopter of the Internet of Things	5 (<0.01%)	2 (<0.01%)			2 (0.02%)
TOTAL	**6**	**3**	**3**	**3**	**2**

The text search on the node, 'enablement' under people factors, is conducted for the word 'train', and the results of the word tree are displayed in Figure 5.40. From here, we can see the factors for cybersecurity awareness to IIoT are training staff, training users, constant training, and the cost to train.

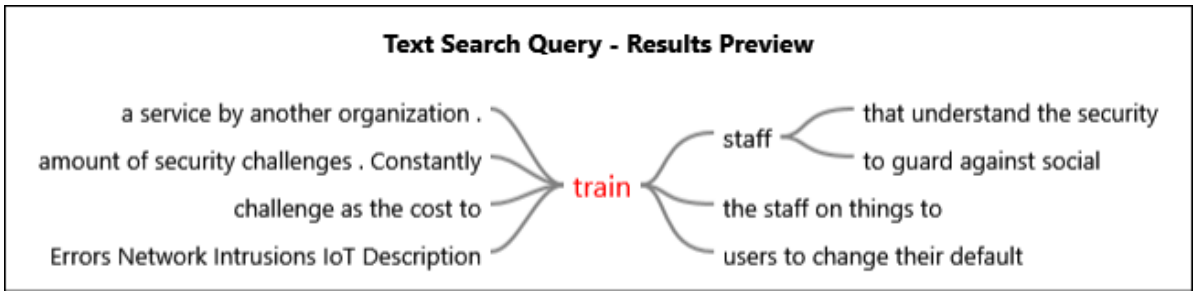


Figure 5-40: Word tree for 'train' under enablement node

The text search on the node, 'enablement' under people factors, is conducted for the words 'human', 'identifiable', 'expertise', and 'staff'. The word tree results are displayed in Appendix C (Figure C73 – Figure C76).

From the analysis of the frequency of nodes for the factor 'enablement', we can conclude that the most prevalent words are:

- **Train**: train staff, train users, constantly train, and cost to train.
- **Expertise**: building up expertise, using their expertise and security engineering expertise.
- **Human**: minimising human error, human understanding, the impact of human understanding, and simplifying for humans.
- **Identifiable**: personally identifiable, identifiable data and identifiable information.
- **Staff**: train staff, cost to train staff, and train staff to guard against social engineering.

Section 6.5.2 discusses the results further, including a unique analysis of the implications for the transport sector.

5.6.3 Employee Engagement

The word frequency for the factor, 'Employee engagement', is visualised in Figure 5.41 and displayed in Table 5.25. The words 'communications' and 'consumer' are most prevalent. Communication is critical to enable staff, and the focus should be on training and upskilling staff. The words following

this in prevalence are: ‘tracking’, ‘people’, and ‘unauthorised’. To gain a clearer understanding of what ‘communications’, ‘consumer’, ‘tracking’, ‘people’, and ‘unauthorised’ are factors of, a text search on the node, ‘employee engagement’ under people factors are conducted and the results displayed in a word tree for each of the most frequent words.

Figure 5-41: Visualisation of the word frequency for Employee engagement to IIoT

Table 5-25: Table of the word frequency for Employee engagement to IIoT

	People – Employee engagement				
Document	**Communications**	**Consumer**	**People**	**Tracking**	**Unauthorised**
Industrial Internet of Things Volume G4 Security Framework					
IoT Trust Framework	3 (0.09%)	3 (0.06%)			
Microsoft – Security Best practices for Internet of Things (IoT)					
NIST					
Security Guidance for Early Adopter of the Internet of Things			2 (<0.01%)	2 (<0.01%)	2 (<0.01%)
TOTAL	**3**	**3**	**2**	**2**	**2**

The text search on the node, ‘employee engagement’ under people factors, is conducted for the word ‘communication’, and the results of the word tree are displayed in Figure 5.42. From here, we can see the factors for employee engagement in IIoT are end-user communications, in-app notifications communications, and communications that should be written.

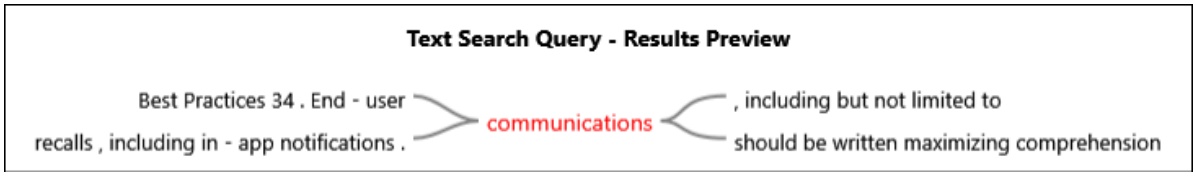


Figure 5-42: Word tree for ‘communications’ under employee engagement node

The text search on the node, ‘employee engagement’ under people factors, is conducted for the word ‘consumer’, and the results of the word tree are displayed in Figure 5.43. From here, we can see the factors for employee engagement in IIoT enable the consumer, consumer notifications and consumer to review and edit privacy.

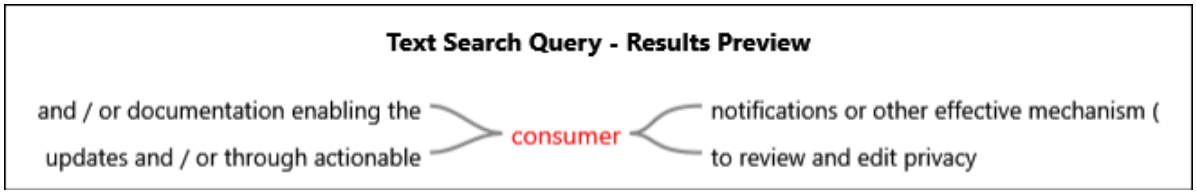


Figure 5-43: Word tree for ‘consumer’ under employee engagement node

The text search on the node, ‘Employee engagement’ under people factors, is conducted for each of the words, ‘tracking’, ‘people’, and ‘unauthorised’. The word tree results are displayed in Appendix C (Figure C77 – Figure C79).

From the analysis of the frequency of nodes for the factor’ Employee engagement, we can conclude that the most prevalent words are:

- **Communication**: End-user communications, in-app notifications communications, and communications should be written.
- **Consumer**: enabling the consumer, consumer notifications and consumer to review and edit privacy.
- **People**: tracking of people’s behaviours and activities and people’s locations.
- **Tracking**: tracking people’s behaviours and activities and tracking people’s locations.
- **Unauthorised**: Unauthorised tracking of people’s behaviours and locations.

Section 6.5.3 discusses the results further, including a unique analysis of the implications for the transport sector.

5.6.4 Employee Satisfaction

The word frequency for the factor, ‘Employee satisfaction’, is visualised in Figure 5.44 and displayed in Table 5.26. The word ‘disclose’ is again most prevalent. Training is critical to enable staff, and the focus should be on training and upskilling staff. The words following this in prevalence are: ‘reward’, ‘motivation’, ‘differing’, ‘effort’, ‘level’, ‘staff’, and ‘system’. To gain a clearer understanding of what ‘disclose’, ‘reward’, ‘motivation’, ‘differing’, ‘effort’, ‘level’, ‘staff’, and ‘system’ are factors of a text search on the node, ‘employee satisfaction’ under people factors are conducted and the results displayed in a word tree for each of the most frequent words.

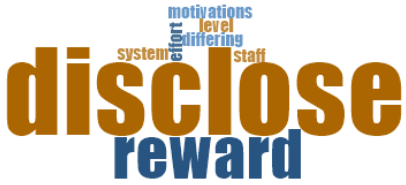


Figure 5-44: Visualisation of the word frequency for Employee satisfaction to IIoT

Table 5-26: Table of the word frequency for Employee satisfaction to IIoT

	People – Employee satisfaction							
Document	**Disclose**	**Reward**	**Differing**	**Motivation**	**Effort**	**Level**	**Staff**	**System**
Industrial Internet of Things Volume G4 Security Framework			1 (<0.01%)	1 (<0.01%)				
IoT Trust Framework	3 (0.06%)							
Microsoft – Security Best practices for Internet of Things (IoT)								
NIST					1 (<0.01%)	1 (<0.01%)		
Security Guidance for Early Adopter of the Internet of Things		2 (<0.01%)					1 (<0.01%)	1 (<0.01%)
TOTAL	**3**	**2**	**1**	**1**	**1**	**1**	**1**	**1**

The text search on the node, 'Employee satisfaction' under people factors, is conducted for the word 'disclose', and the results of the word tree are displayed in Figure 5.45. From here, we can see the factors for Employee satisfaction with IIoT are disclosing if and how IoT devices, the data retention policy, and what and how.

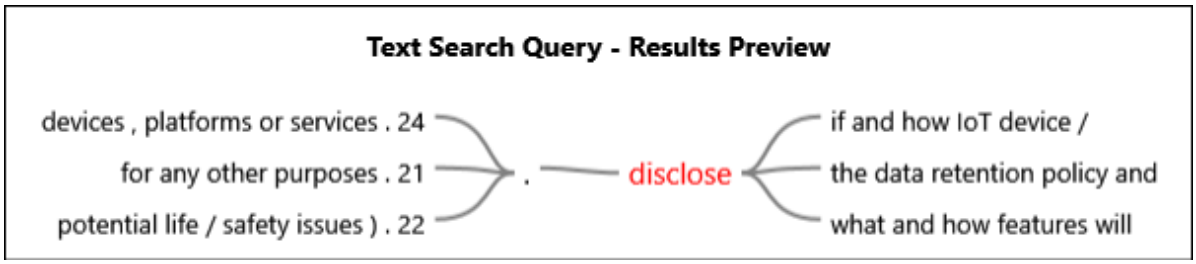


Figure 5-45: Word tree for 'disclose' under employee satisfaction node

The text search on the node, ‘Employee satisfaction’ under people factors, is conducted for each of the words, ‘reward’, ‘motivation’, ‘differing’, ‘effort’, ‘level’, ‘staff’, and ‘system’. The word tree results are displayed in Appendix C (Figure C80 – Figure C86).

From the analysis of the frequency of nodes for the factor ‘Employee satisfaction, we can conclude that the most prevalent words are:

- **Disclose**: Disclose if and how IoT devices, the data retention policy, and what and how.
- **Reward**: reward system gives people initiative and rewards the staff.
- **Differing**: a balance consideration of their differing motivations.
- **Motivation**: Balance consideration of their differing motivations.
- **Effort**: level of effort needed to manage.
- **Level**: level of effort needed to manage.
- **Staff**: Reward the staff when they find vulnerabilities.
- **System**: A reward system gives people the initiative to report.

Section 6.5.4 discusses the results further, including a unique analysis of the implications for the transport sector.

5.7 Shodan

Project SHINE (2014) released a report in 2014 that contained information on ICS/SCADA devices that are directly connected to the Internet. This was used to produce results for IIoT in South Africa. From Section 2.3.2.5, the most common protocols and ports used that are Internet-facing and uniquely to IIoT are MQQT, AMQP, CoAP and DDS. Although IIoT also uses protocols like Ethernet, Wi-Fi and Cellular, it would be challenging to distinguish between IIoT devices and ICT devices. Hence these are excluded.

The open-source search engine, Shodan (www.shodan.io), is used to search for these protocols to determine the number of IIoT devices in SA that are exposed to the Internet. There are 1,339 IIoT devices in SA exposed to the Internet. Appendix D summarises the results.

It is impossible to identify if these IIoT devices are vulnerable and pose a risk without additional vulnerability scans, control testing, or ethical penetration tests. Moreover, it is difficult to determine to which sector these devices belong to based on their IP address. Therefore, these results were excluded from the study.

5.8 Summary

The document analysis is conducted on cybersecurity standards, frameworks, and best practices. Qualitative analysis of cybersecurity standards, frameworks and best practices is conducted through thematic and content analysis. Five documents are selected based on the relevance and percentage of responses from the questionnaires. They are NIST: IR.8228 Consideration for Managing IoT Cybersecurity and Privacy Risks, Microsoft: Internet of Things security best practices, Cloud Security Alliance: Security Guidance for Early Adopters of the Internet of Things (IoT), IIC: Industrial Internet of Things, Volume G4: Security Framework and Online Trust Alliance: IoT Trust Framework. The prevalent themes in the documents are provided via thematic analysis, indicating the relationships between the various documents and research objectives. These will be used to guide the development of the cybersecurity framework in Section 6.7.3

The results from this chapter (qualitative analysis) are used to triangulate the results from the previous chapter (Chapter 4) and provide input into the development of controls in the cybersecurity framework in Section 6.7.3.

The next chapter discusses the results from the quantitative and qualitative analysis and link them back to the study's objectives to draw meaningful outcomes. The results from the quantitative and qualitative analysis are also used to develop a cybersecurity framework to address the gaps identified.

Chapter 6 Discussion

6.1 Introduction

Chapter 4 presented the results and outcomes of the online questionnaire (quantitative data), and Chapter 5 the findings from document analysis (qualitative data). This chapter revisits the study's objectives and discusses the findings and results per research objective and impact on the transport sector. The results are also triangulated and discussed in line with the results from the document analysis to draw meaningful implications and comparisons to international studies. Figure 6.1 is a graphical representation of the outline of this chapter and overall structure. The research objectives are listed in Table 6.1 and the study's outcomes in line with each objective follow.

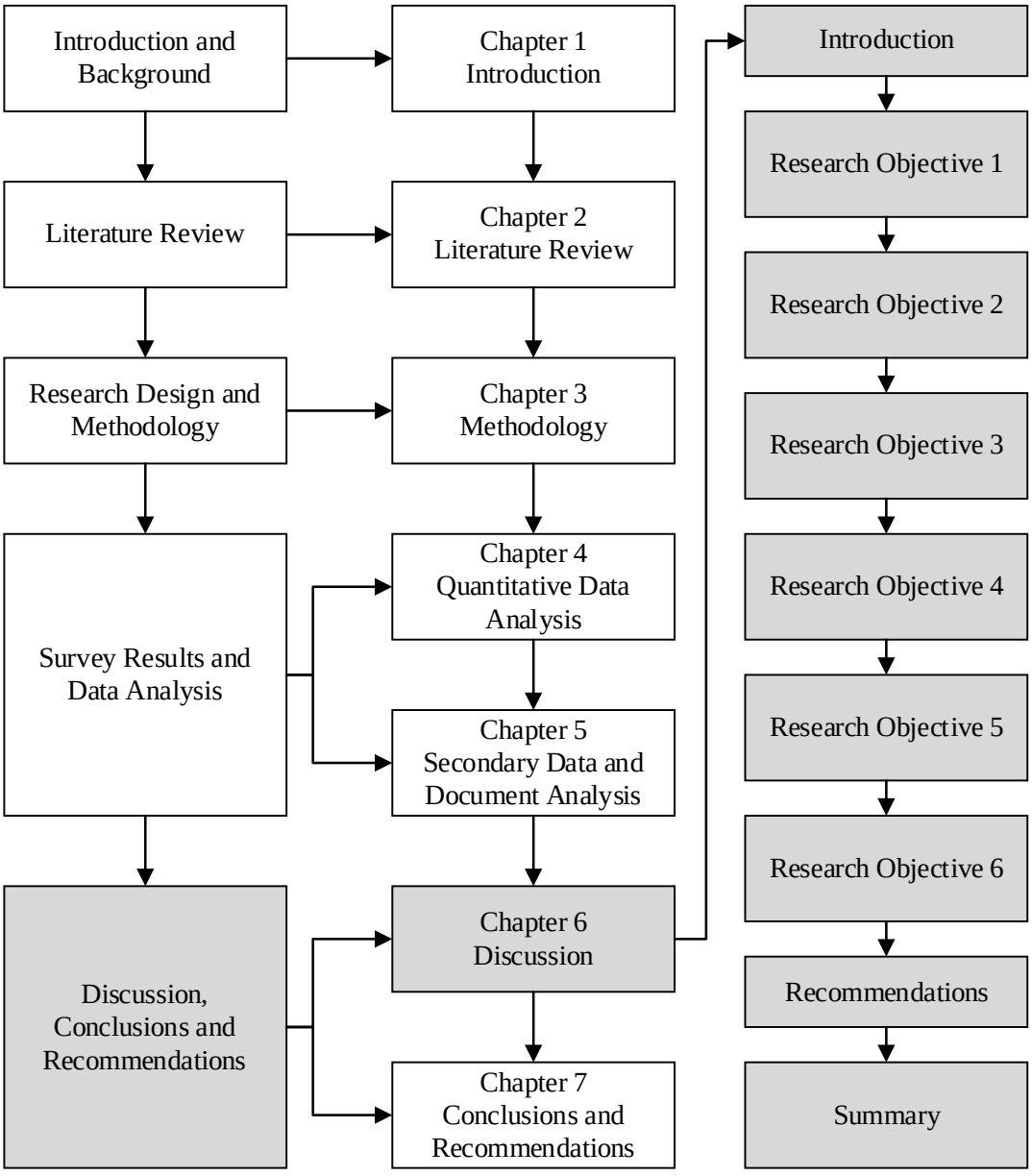


Figure 6-1: Graphical representation of Chapter 6 outline

Table 6-1: Summary of Research objectives

	Research objective	Section
RO1	To determine the extent to which the technological factors influence IIoT cybersecurity in the SA transport sector: • Existing and new threats due to IIoT • Vulnerabilities • Risks	**6.2**
RO2	To critically assess the organisational factors influencing IIoT cybersecurity in the SA transport sector: • Size and structure • Cybersecurity strategy • Risk appetite • Innovativeness culture • Security culture • Senior executive engagement with security	**6.3**
RO3	To critically assess the procedural factors influencing IIoT cybersecurity in the SA transport sector: • Security incident response • Risk management • IT governance and compliance • Policies, standards, and procedures • Legal and regulatory requirements	**6.4**
RO4	To assess the extent of the people factors influencing IIoT cybersecurity in the SA transport sector: • Cybersecurity awareness • Enablement • Employee engagement • Employee satisfaction	**6.5**
RO5	To assess the degree of the relationships amongst the BMIS factors for IIoT cybersecurity in the SA transport sector.	**6.6**
RO6	To develop and validate a cybersecurity framework for IIoT in the SA transport sector using the data collected.	**6.7**

6.2 Research Objective 1 – To determine the extent to which the Technological Factors Influence IIoT Cybersecurity in the South African Transport Sector

This objective aimed to determine the factors (existing and new threats due to IIoT, vulnerabilities and risks) influencing IIoT cybersecurity in the SA transport sector. Results from the quantitative data (questionnaire) analysis and document analysis are discussed in the sections below.

6.2.1 Existing and New Threats due to IIoT

It is noted in Section 4.3.1 of the questionnaire that the threats (existing and new) likely to be introduced by IIoT in the transport sector in SA are:

- Remote access.
- Cyber espionage.
- Ransomware.

The results are triangulated to the question in Section 4.3.2 as the respondents listed the top 3 threats as malware (worms, viruses, trojans or spyware), insider and privilege misuse, and combined third

DDoS and cyber espionage. Cyber espionage is closely linked to insider and privilege misuse identified from the questionnaire as threats likely to be introduced by IIoT, and ransomware identified from the questionnaire as threats likely to be introduced by IIoT is part of the malware grouping.

From the document analysis in Section 5.3.1, it is evident that the most prevalent threats (existing and new) likely to be introduced by IIoT are access (remote access), malicious (malicious code or application, i.e., malware), attacks (denial of service attacks), and privileged access, which include privilege misuse. These are aligned to the top threats mentioned above and in Section 4.3.1 and Section 4.3.2. The top three threats for general IIoT, as discussed in Section 2.4.5 are DDoS, malware, and botnets. There are some overlaps between the first two and the results from the quantitative data.

From Figure 6.2, we can see that malware appears across all the results. This is because malware is one of the most common attack vectors (Fleury, Dubrunquez, & Alouani, 2021). DDoS appears in most of the results. Cyber espionage only appears in the results from the quantitative data analysis and quantitative data selected by the respondents. This makes it unique to the transport sector as it does not appear under the general IIoT threats discussed in Section 2.4.5.

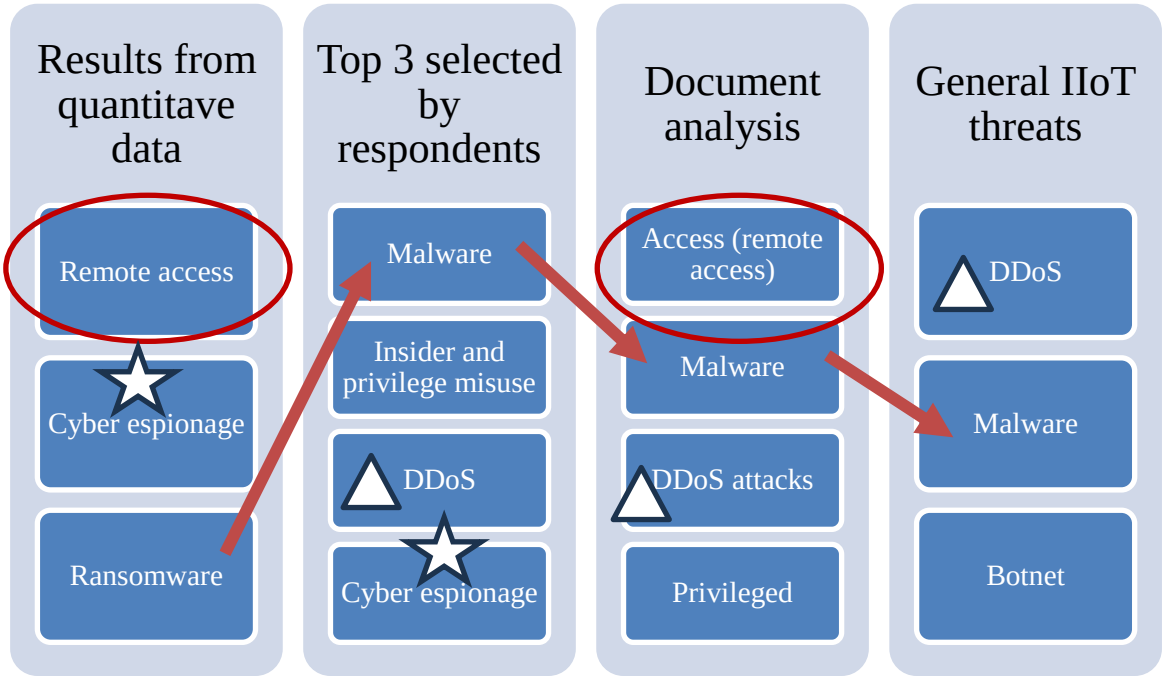


Figure 6-2: Triangulation of threats

Legend	Details
	Showing similarities for remote access
	Showing similarities for malware

Legend	Details
	Showing similarities for DDoS
	Showing similarities for cyber espionage

The threats above have the following impact on the transport sector of South Africa:

- **Remote Access**: In an IIoT-enabled transportation system, remote access is crucial for monitoring, control, and maintenance (Burkhalter, 2022b; Kapkaeva et al., 2021; KVH Watch, 2021). However, unauthorised remote access poses a significant threat, as it can lead to disruptions, unauthorised control, and potential compromise of operational efficiency. This was starkly demonstrated in the case of the Maroochy Water System, an Australian sewerage company, where a disgruntled employee of the controller supplier obtained remote access and intentionally released sewerage into the waterways, aiming to secure a job with the municipality (Abrams & Weiss, 2008; Wyld, 2004). While this incident is unrelated to the transport sector, it serves as a powerful example of the impact that unauthorised remote access can have on a business, highlighting the relevance of this threat to the transport sector of South Africa.
- **Cyber espionage**: As discussed earlier, this threat is unique to IIoT in the transport sector as compared to general IIoT threats. The transport sector, a vital part of a nation's infrastructure, often characterized by advanced technology such as IIoT, is a prime target for industrial cyber espionage (Maxime, Tibirna, & TDR, 2024). This threat is particularly relevant within the civil aerospace industry, especially among airliner manufacturers, due to their significant research and development investments (Maxime et al., 2024). Cyber espionage targeting IIoT systems can result in the theft of sensitive information, which could have profound implications for national security, economic stability, and competitiveness, as demonstrated by the capabilities of the Flame malware used for cyber espionage (Nakashima & Warrick, 2012; Nakashima, Miller, & Tate, 2012; Rodionov, 2012). This underscores the seriousness of the threat to South Africa's transportation sector. Various cybersecurity vendors frequently report intrusion sets associated with China, such as LanceFly, APT41, Winnti, and Mustang Panda, as actively engaged in industrial cyber espionage, with a notable focus on aerospace companies (Maxime et al., 2024). For instance, APT41, a group linked to the Chinese Ministry of State Security, was first observed by TrendMicro in March 2022, utilising a customized Cobalt Strike loader to target a Taiwanese aviation firm. This aligns with the victimology analysis conducted by Symantec and Recorded Future on LanceFly, an intrusion set that exhibits technical overlaps with APT41 (Symantec Threat Hunter Team, 2023).

- **Malware (Ransomware)**: Malware, particularly ransomware, can compromise the integrity of IIoT systems. In transportation, this can lead to disruptions in traffic control and logistics and potentially compromise the safety of passengers and cargo, posing direct risks to human lives and property. The increase in ransomware, as evidenced by the cases of Maersk and Transnet in the transportation sector of SA (discussed in Section 2.4.7.1), underscores the urgency of implementing effective cybersecurity measures to mitigate these threats.
- **Insider and Privilege Misuse** Insiders with malicious intent or individuals exploiting their privileges can significantly threaten IIoT systems in the transport sector. This threat extends to data manipulation, unauthorised access to critical systems, potential sabotage, and criminal activities. As discussed in Section 2.4.7.1.1, cybercriminals smuggled goods into the Port of Antwerp in 2013 using cyberattacks to track shipping containers (Dunn, 2013). Insider threats refer to the possibility of insecure rogue devices breaching security; insider threats were listed as one of the major categories of cyber incidents in 2019 (McKee, 2019).
- **DDoS**: DDoS attacks can overwhelm IIoT networks, disrupting communication and data transfer. This can lead to service outages in the transportation sector, impacting scheduling, real-time communication, and coordination, as seen in multiple incidents discussed in Section 2.4.7.1.1.

Within the transportation sector, there is a prevalence of IoT in terms of smart TVs for boardrooms and CCTV systems; however, the second most prevalent devices relate to IIoT and are used for ICS/SCADA, vehicle tracking/monitoring, industrial controllers (e.g., PLCs) sensors and cargo tracking. The smart TVs and CCTV systems are of particular note, mainly due to concerns of eavesdropping via the smart TVs and the use of CCTV systems in the notorious Mirai botnet used to conduct DDoS attacks. The availability of IIoT devices used in ICS/SCADA, vehicle tracking/monitoring, and industrial controllers (e.g., PLCs) sensors are critical to operations and unavailability because threats such as DDoS attacks or malware could seriously compromise operations and have a financial impact. Two of the top three perceived threats are therefore aligned to these specific IIoT devices: cyber espionage relating to the TVs and IIoT devices and network unavailability relating to the possibility of DDoS due to compromised IIoT devices.

It is noted in Section 4.3.8 of the questionnaire that 29% of respondents indicated that a threat did occur, and 26% of respondents did not have a threat occur in their IIoT environment in the transport sector of South Africa. 25% were unsure while 11% indicated there might have been a threat, while 9% couldn't disclose. From this, it could be concluded that only 26% did not have a threat occur in their IIoT environment. The remaining 74% might have had a threat in their IIoT environment. This strengthens the need to secure IIoT systems, as 74% of respondents might have a threat occur in their IIoT environment. Furthermore, the questionnaire was sent to respondents before cyberattacks on

significant transportation companies in South Africa, namely Transnet, refer to the discussion in Section 2.3.7.1.1 It is noted in Section 4.5.5 that over 50% of the respondents are not confident in the controls they implemented to mitigate the threats and risks. This further strengthens the need to secure IIoT systems in the transportation sector of South Africa.

The factors, existing and new threats due to IIoT influencing IIoT cybersecurity in the SA transport sector are remote access, cyber espionage, malware (particularly ransomware), insider and privilege misuse, and Distributed Denial of Service (DDoS).

6.2.2 Vulnerabilities

It is noted in Section 4.3.3 from the questionnaire that the three vulnerabilities related to IIoT environment in the transportation sector of SA are:

- No patching or firmware updates or delays thereof.
- Insecure default settings.
- Insecure mobile interface.

From the document analysis in Section 5.3.2, it is evident that the most prevalent vulnerabilities for IIoT are: legacy endpoints or devices, legacy communications or protocols, and poor physical security.

Legacy and out-of-date security relate to no patching or delay in patching/firmware updates, incorrect security configurations relate to insecure default settings, and insecure interfaces (e.g., mobile, web and API) to insecure mobile interfaces. This strengthens and aligns the vulnerabilities mentioned in the questionnaire with the vulnerabilities in the analysis of the documents.

The type of IIoT devices in the transport sector in SA from Section 4.3.9 it is noted that 80% of the respondents have boardroom/video conferencing equipment, 74% have CCTV / Smart cameras, 58% have vehicle tracking/monitoring, 54% also have sensors (general), 51% have IIoT devices for cargo tracking, 48% have industrial Wi-Fi / LTE. In comparison, 46% have environmental monitoring devices (e.g. weather, wind, fire detection), equipment monitoring, cargo monitoring (e.g. reefer monitoring, status of cargo), and building management systems (e.g. aircon controllers), 43% have equipment tracking, 40% have smart metering (e.g. energy monitoring), only 9% have smart parking and IIoT devices for traffic flow management.

All the perceived vulnerabilities are linked to the concept of insecure-by-design, where products are supplied without sufficient security testing or undisclosed bugs (Solomon, 2022). These vulnerabilities can allow malicious users to easily compromise IIoT devices to gain a foothold in a network, as demonstrated by several incidents discussed in Section 2.4.6 and Section 2.4.7.1.

The vulnerabilities above have the following impact on the transportation sector of South Africa:

- **No or delay in patching**: The transportation sector relies heavily on interconnected systems, and any delay or absence in applying security patches or firmware updates can expose vulnerabilities. Without timely updates, transportation systems become susceptible to exploitation by cyber threats, jeopardizing operational continuity and system integrity, as seen in the incidents in Section 2.3.6 and Section 2.3.7.1.
- **Insecure default settings**: Many IIoT devices come with default settings that may not be secure (Barrett, 2022). In the transportation sector, insecure default settings can be exploited by malicious actors to gain unauthorised access, manipulate configurations, or disrupt normal operations. Addressing and securing default settings are crucial for preventing unauthorised access and maintaining the overall cybersecurity posture. This is apparent, as illustrated by the casino fish tank incident discussed in Section 2.3.6, wherein a vulnerable single connected temperature sensor served as an entry point into the network, resulting in the theft of 10GB of data (Schiffer, 2017). Equipment in the transportation sector has more than one IIoT device, which increases the attack surface if they are misconfigured or vulnerable.
- **Insecure Mobile Interface**: The transportation industry increasingly relies on mobile interfaces for monitoring and control (Oladimeji et al., 2023). Insecure mobile interfaces can serve as entry points for cyberattacks, allowing adversaries to compromise systems, access sensitive data, or disrupt operations. Securing mobile interfaces is vital for protecting against unauthorised access and ensuring the confidentiality and integrity of data.
- **Legacy endpoints or devices:** Legacy endpoints and devices, which may need more modern security features, pose a significant risk to IIoT cybersecurity. In the transportation sector, outdated systems may be more susceptible to exploitation, making it easier for attackers to compromise critical infrastructure (QC Staff, 2023). Upgrading or replacing legacy devices is essential for maintaining a robust and secure IIoT environment.
- **Legacy communications or protocols:** Older communication protocols may need more robust security features for modern cybersecurity standards. Relying on legacy communication protocols exposes systems to potential interception, manipulation, or unauthorised access in the transportation sector (QC Staff, 2023). Transitioning to secure and modern communication protocols is crucial for safeguarding data integrity and confidentiality.

According to the findings discussed in Section 5.9, numerous IIoT devices located in SA have been exposed to the Internet. Unfortunately, it remains uncertain whether these devices are susceptible to vulnerabilities or which sector they pertain to. As a result, these findings were omitted from the study. Future investigations may consider implementing a honeypot that mimics an IIoT device to examine potential weaknesses and modes of attack.

The vulnerability factors influencing IIoT cybersecurity in the SA transport sector are no or delay in patching/firmware updates, insecure default settings, insecure mobile interface, legacy endpoints/devices, and legacy communications/protocols.

6.2.3 Risks

The safety risk (human safety, safety regulations/considerations/consequences/implications) relates to the top risk of the unavailability of IIoT devices or networks, as these would directly impact safety should these systems be compromised. Both data (data to unauthorised parties, data exfiltration and leaks) and information (information disclosure and stolen information) relate to the risk of cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information. They would also have an impact on reputation. This aligns with the top three risks discussed, the spyware attacks discussed in Section 2.2.7.7 and strengthened consistency across all analysis sets and results showing high confidence levels.

The risks above have the following impact on the transportation sector of South Africa:

- **Unavailability of IIoT devices or networks**: The unavailability of IIoT devices or networks in the transportation sector can disrupt essential operations, leading to service outages, delays, and potential safety concerns. This risk factor underscores the need for robust infrastructure and contingency plans to ensure continuous availability and functionality.
- **Damage to reputation**: The transportation sector relies heavily on public trust (Pagliara, Aria, Russo, & Corte, 2021). Cybersecurity incidents resulting in system compromises or data breaches can damage the reputation of transportation services. A damaged reputation may lead to a loss of customer trust, reduced ridership, and adverse economic implications for the industry. This is evident in reputational damage suffered after incidents suffered by Transnet and Maersk, discussed in Section 2.3.7.1.1.
- **Cyber espionage compromising trade secrets and sensitive Information**: The transportation sector often deals with sensitive information related to trade secrets, research and development, and other proprietary data. Cyber espionage poses a significant risk, as compromising such information can lead to economic losses, decreased competitiveness, and potential threats to national security. This aligns with the cyber espionage threat discussed in Section 6.2.1, with the risk of compromised trade secrets and sensitive information and the effect on the transport sector.
- **Human Safety**: The direct impact of IIoT cybersecurity breaches on human safety is a critical risk factor. Compromised transportation systems can lead to accidents, disruptions in traffic control, and unsafe conditions for passengers and personnel. Ensuring the cybersecurity of IIoT devices is paramount to safeguarding human lives. This is evident in the train incident discussed in Section 2.4.7.1.2, in which 12 people were hurt.

- **Safety regulations (considerations, consequences, and implications)**: The transportation sector is subject to strict safety regulations (Cheit, 1990). IIoT cybersecurity incidents can have legal consequences, financial penalties, and implications for compliance with safety standards. Managing cybersecurity risks is essential to avoid regulatory non-compliance and associated consequences.

Section 4.5.5 notes that when asked how confident the respondents are that the controls mitigate the threats and risks. 35% indicated that they are somehow confident, 28% are not confident at all, 25% are moderately confident, 11% are confident, and only 1% are *v*ery confident. This indicates that over 50% of the respondents need more confidence in the controls they implemented to mitigate the threats and risks.

The risk factors Influencing IIoT cybersecurity in the SA transport sector are the unavailability of IIoT devices or networks, damage to reputation, cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information, human safety, and safety regulations (considerations, consequences, and implications).

6.3 Research Objective 2 – To critically assess the Organisational Factors Influencing IIoT Cybersecurity in the South African Transport Sector

This objective aimed to assess the organisational factors (Size and structure, Cybersecurity strategy, Risk appetite, Innovativeness culture, Security culture, and Senior executive engagement with security) influencing IIoT cybersecurity in the SA transport sector. Results from the quantitative data (questionnaire) analysis and document analysis are discussed below.

Six organisational factors influence IIoT cybersecurity in the SA transport sector: size and structure, cybersecurity strategy, risk appetite, innovativeness culture, security culture, and senior executive engagement with security.

From the analysis in Section 4.4, we noted that the number of IT staff supporting IIoT in the transport sector of SA is limited, with an even more constrained number dedicated to security roles and IIoT security roles. There is a massive gap in the IIoT security staffing as most staff are allocated as part of a project rather than dedicated to IIoT security.

The following organisational factors for an IIoT environment in the transport sector of SA all have a maturity that is managed, indicating the process is characterised for projects and is often reactive:

- The cybersecurity roadmap/strategy.
- The risk appetite.
- The innovativeness culture and

- The senior or executive management has an understanding of IIoT security.

The document analysis in Section 5.4 notes the main phrases or prevalent words from the IIoT documents. These demonstrate basic security principles applied to IIoT and will guide the development of the control framework in Section 6.7.3. The main phrases or prevalent words for each factor are displayed in Figures 6.3 and 6.4.

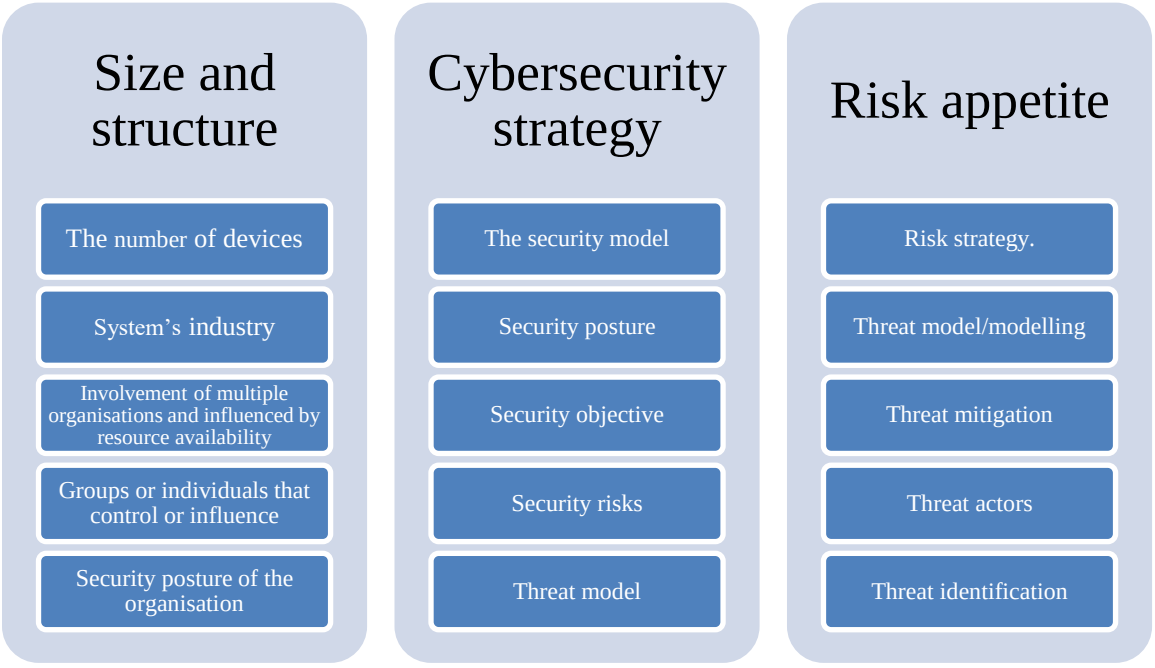


Figure 6-3: Main phrases for size and structure, cybersecurity strategy and risk appetite

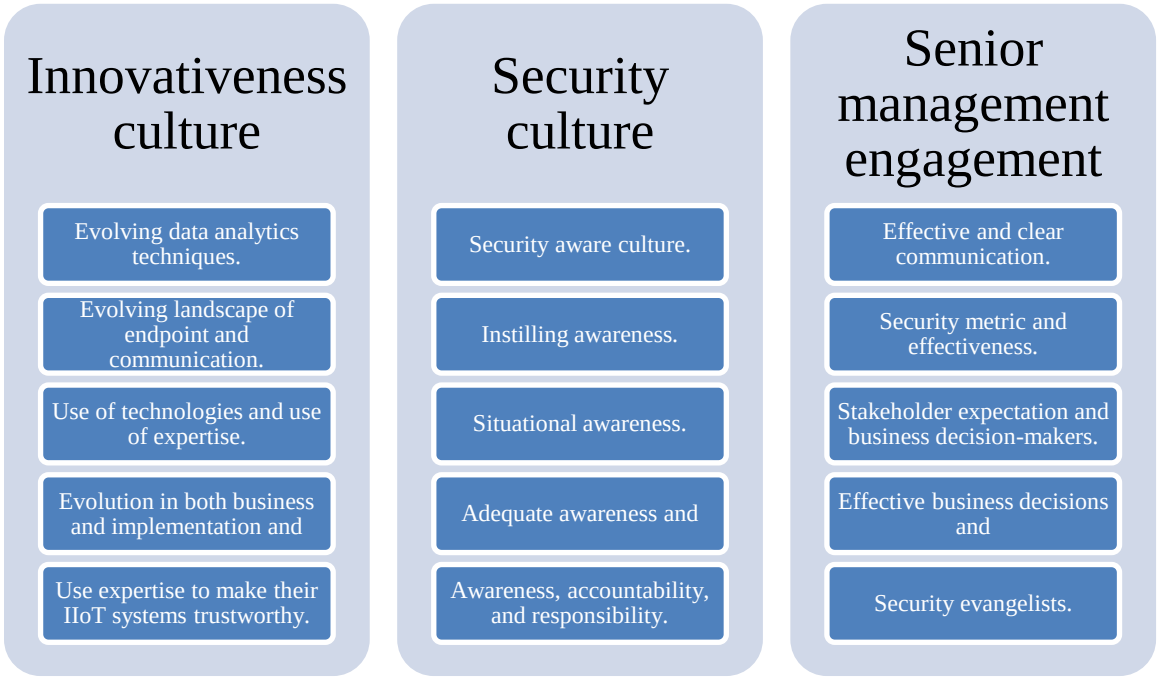


Figure 6-4: Main phrases for innovativeness culture, security culture and senior management engagement

The factors above have the following impact on the transportation sector of South Africa, as discussed in Section 6.31 – Section 6.3.6.

6.3.1 Size and Structure

Larger organisations with complex structures may face challenges implementing cohesive cybersecurity measures across various departments and divisions (Hirsch, 2019). Conversely, smaller organisations may have limited resources dedicated to cybersecurity, making them more vulnerable to cyber threats. From the analysis in Section 4.2.3, we saw that over 70% of respondents work at a company with over 5,000 employees. This size factor makes implementing cybersecurity measures more difficult across the organisation, and combining this with a shortage of cybersecurity staff, the transportation sector becomes more vulnerable to cyber threats targeting IIoT systems. This could include attacks aimed at disrupting operations, stealing sensitive data, or compromising safety-critical systems, as discussed in Sections 6.21 – 6.2.3.

The need for more staff to support IIoT could also force transport companies to make difficult decisions regarding resource allocation. Limited resources may be spread thin across various operational areas, potentially compromising cybersecurity, and efficiency. This was seen in the delays experienced by Transnet towards the end of 2023 (Opperman, 2023).

The need for more staff supporting IIoT may impede innovation within the transport sector. With limited resources available for developing and implementing new IoT technologies, transportation companies may need help to keep up with competitors and meet evolving customer demands (Kumar, Sindhwani, & Singh, 2022).

More personnel dedicated to IIoT security increases the risk of data breaches within the transport sector. Given the sensitive nature of transportation data, such breaches could lead to financial losses, disruptions, and damage to reputation, as discussed in Section 6.2.3.

The key phrases that will guide the development of the cybersecurity framework related to the size and structure of IIoT security staff are determined by the number of devices, the system's industry, and the involvement of multiple organisations. They are influenced by resource availability, groups or individuals that control or influence, and the organisation's security posture.

6.3.2 Cybersecurity Strategy

Organisations with well-defined cybersecurity strategies are better equipped to identify, assess, and mitigate cyber risks associated with IIoT deployments (Boye, 2021), but they also have the power to steer their cybersecurity initiatives effectively and respond promptly to emerging threats. A robust cybersecurity strategy serves as a compass, guiding investment decisions, resource allocation, and the implementation of cybersecurity controls (Boye, 2021). This, in turn, enhances the overall resilience

of IIoT systems in the transportation sector. IIoT systems are left vulnerable to cyber threats without a robust cybersecurity roadmap, as discussed in Section 6.2.1. These systems, often comprising interconnected devices and networks, as mentioned in Section 2.4.2, create numerous potential entry points for attackers. On the other hand, an immature strategy may need more essential security controls and adequately address emerging threats, thereby putting critical transport infrastructure and sensitive data at risk.

Inadequate cybersecurity measures increase the likelihood of data breaches and intellectual property theft, as seen through cyber espionage in Section 6.21 and Section 6.2.3. IIoT environments often handle sensitive information, such as operational data, customer records, and proprietary technology (Sha, Xiao, Chen, & Sun, 2018). A lack of proper security controls can expose this data to unauthorised access, leading to financial losses, disruptions, and damage to reputation, as discussed in Section 6.2.3.

The key phrases that will guide the development of the cybersecurity framework related to the cybersecurity roadmap/strategy of IIoT are the security model, security posture, security objective, security risks, threat model, and cybersecurity capability maturity model and influenced by business decisions, business needs, business objectives and risk strategy, business priorities, business sectors and verticals risk appetite of the organisation.

6.3.3 Risk Appetite

Organisations with a high-risk appetite may prioritise innovation and operational efficiency over cybersecurity, potentially exposing IIoT systems to more significant security vulnerabilities (Boye, 2021). The organisation's risk appetite influences decision-making processes, investment strategies, and tolerance levels for cybersecurity risks associated with IIoT initiatives in the transportation sector (Boye, 2021). This can lead to a lax approach to security controls and inadequate investment in cybersecurity measures, increasing the likelihood of security incidents and breaches and regulatory penalties (Paloika & Klubnikin, 2023). An immature risk appetite may result in underestimating or overlooking cybersecurity risks associated with IIoT deployments in the transport sector. This can leave organisations vulnerable to a wide range of cyber threats, as discussed in Section 6.2.1.

The key phrases for risk appetite of IIoT that will guide the development of the cybersecurity framework is determined by the risk strategy (e.g. risk avoidance, risk acceptance, outsourcing of risk, risk transfer and risk mitigation), threat model/modelling, threat mitigation, threat actors, threat identification, and impact of unavoidable threat and influenced by replacement cost, cost of an incident/consequence; mitigation exceeds the cost, the balance of cost, cost of upgrading security, and cost versus effectiveness of security controls, business risk/risks, business objectives, business priorities and business sectors.

6.3.4 Innovativeness Culture

Organisations with a strong culture of innovation are more likely to embrace new technologies and explore innovative use cases for IIoT in the transportation sector (Ghosh, Hughes, Hodgkinson, & Hughes, 2022). However, this culture of innovation may also introduce new cybersecurity challenges as organisations strive to stay ahead of competitors by rapidly deploying new technologies without adequate security measures (Ghosh et al., 2022). Balancing innovation with cybersecurity requires organisations to foster a culture of responsible innovation, where cybersecurity considerations are integrated into developing and deploying IIoT solutions.

6.3.5 Security Culture

A strong security culture promotes cybersecurity awareness, accountability, and best practices among employees at all levels of the organisation (Uchendu, Nurse, Bada, & Furnell, 2021). Conversely, a weak security culture may lead to complacency, negligence, and inadvertent security breaches that could compromise IIoT systems in the transportation sector. Cultivating a security-conscious culture through training, education, and awareness programs enhances the organisation's resilience to cyber threats and strengthens its overall cybersecurity posture.

An immature security culture may result in a need for more awareness and understanding of cybersecurity risks among transport sector employees (Uchendu et al., 2021). This can lead to careless activities, such as weak password management, failure to patch, and exposure to social engineering attacks, increasing the organisation's vulnerability to cyberattacks targeting IIoT systems.

Organisations needing a mature security culture may need to pay more attention to security best practices and controls when deploying and managing IIoT systems (Uchendu et al., 2021). This can result in inadequate security controls, unpatched systems, poorly configured devices, insecure mobile interfaces, and insufficient safeguards to protect against cyber threats, as discussed in Section (6.2.2), leaving IIoT deployments vulnerable to exploitation and compromise.

6.3.6 Senior Executive Engagement with Security

Active involvement and support from senior executives are critical for driving cybersecurity initiatives and establishing a security culture within the organisation (Uchendu et al., 2021). Without visible leadership and commitment to cybersecurity, IIoT projects may lack the necessary resources, prioritisation, and organisational buy-in to address security risks effectively.

Senior executive engagement with security influences the organisation's strategic direction, resource allocation, and commitment to cybersecurity governance, ultimately shaping the organisation's ability to mitigate cyber risks associated with IIoT deployments in the transportation sector.

6.4 Research Objective 3 – To critically assess the Procedural Factors Influencing IIoT Cybersecurity in the South African Transport Sector

This objective aimed to assess the procedural factors (Security incident response, Risk management, IT governance and compliance, Policies, standards and procedures and Legal and regulatory requirements) influencing IIoT cybersecurity in the SA transport sector. Results from the quantitative data (questionnaire) analysis and document analysis are discussed in the section below.

Five procedural factors influence IIoT cybersecurity in the SA transport sector: security incident response, risk management, IT governance and compliance, policies, standards and procedures, and legal and regulatory requirements.

From the analysis in Section 4.5, we noted that the organisational incident response plan is more mature than the incident response plan in addressing risks in the IIoT environment. The incident response plan for the IIoT environment is below managed, indicating the process is characterised for projects and is often reactive. This indicates that although organisations in the transport sector have an incident response plan, it does not sufficiently address the IIoT risk.

While the general security policies/procedures implemented for an IIoT environment in the transport sector of SA are between managed and defined, the following procedural factors all have a managed maturity, indicating the process is characterised for projects and is often reactive:

- Risk management.
- Governance processes for general IT environment.
- IIoT security policies/procedures/controls implemented.
- Governance processes for IIoT.
- Control framework for IIoT.

The legal and regulatory requirements for an IIoT environment in the transport sector of SA are one of the top three (3) priorities.

From Section 4.5.4, we noted that most respondents either rely on staff to know when to search for events or review audit logs to detect threats. About a third use anomaly detection tools (SIEM/SIC) to identify trends or third-party intelligence. Detection of threats or anomalies is critical to ensure timely resolution as discussed in Section 2.2.3.1.

The top three frameworks used by the respondents to govern and secure their IIoT environments in the transport sector of SA are:

- COBIT.
- ISO 27001 series and

- NIST.

COBIT is suitable from a governance and security perspective. However, ISO 27001 and NIST are more suitable as they focus more on security. This aligns with the maturity of general security policies and procedures implemented for an IIoT environment in the transport sector of South Africa, as COBIT is more of a general governance and security framework and is the one primarily implemented. Implementing general security policies and procedures is more mature than the maturity of the IIoT security policies, procedures, and controls.

The document analysis in Section 5.5 notes the main phrases or prevalent words from the IIoT documents. These demonstrate basic security principles applied to IIoT and will guide the development of the control framework in Section 6.7.3. The main phrases or prevalent words for each factor are displayed in Figures 6.5 and 6.6.

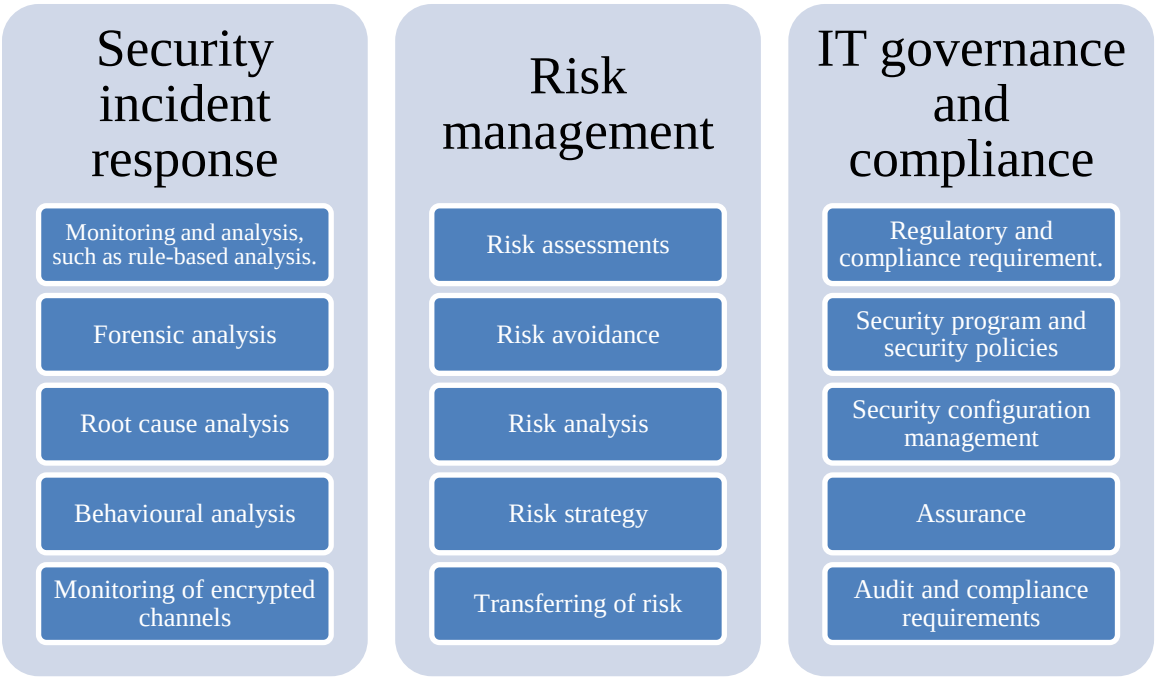


Figure 6-5: Main phrases for security incident response, risk management and IT governance

The factors above have the following impact on the transportation sector of South Africa as discussed in Section 6.4.1 – Section 6.4.5.

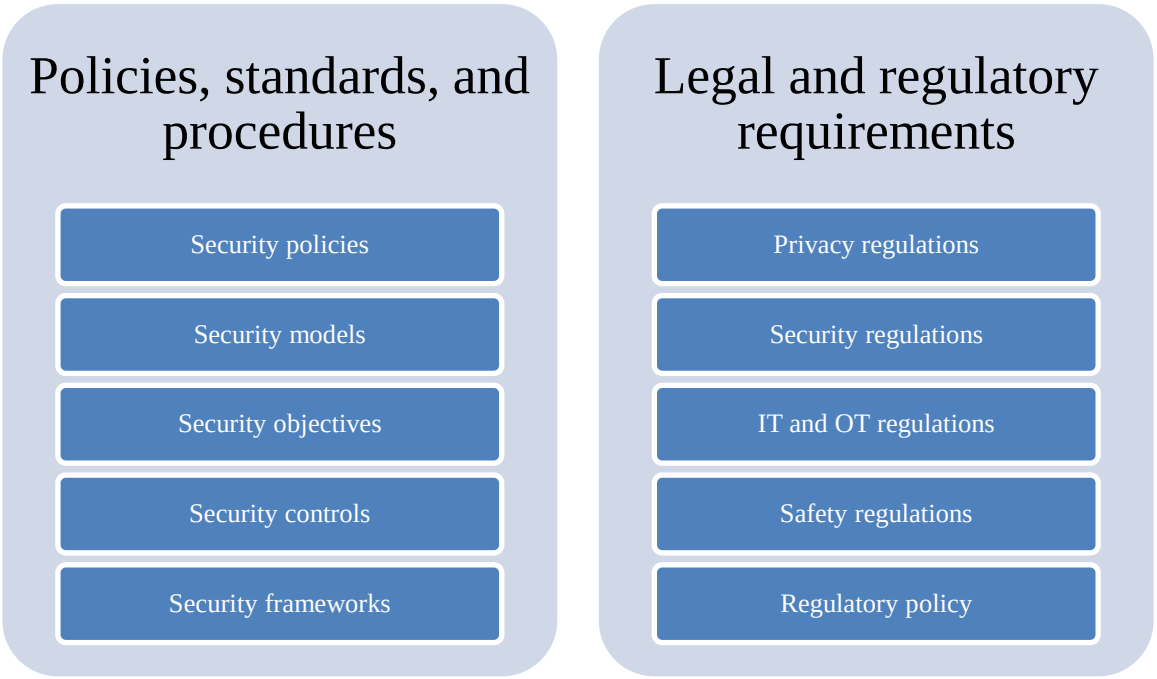


Figure 6-6: Main phrases for policies, standards, procedures and legal and regulatory requirements

6.4.1 Security Incident Response

Effective security incident response procedures are crucial for minimising the impact of cyberattacks and mitigating disruptions to operations (Irei & Shea, 2024). The results indicated that an organisation in the transport sector of South Africa's incident response plan does not address the IIoT risk sufficiently. By adequately addressing the IIoT risk through the incident response plans and timely detection and response mechanisms in place, IIoT systems are protected from prolonged downtime, data breaches (Irei & Shea, 2024), and threats mentioned in Section 6.2. This could lead to the unavailability of IIoT devices and networks, damage to reputation and possible compromise of trade secrets and sensitive information, as mentioned in Section 6.2.3.

Prompt and coordinated incident response efforts can help organisations minimise cybersecurity incidents' financial, operational, and reputational consequences (Irei & Shea, 2024), ensuring the continuity and resilience of transportation services in South Africa.

6.4.2 Risk Management

Comprehensive risk management processes are essential for identifying, assessing, and mitigating cybersecurity risks (NIST, 2019) associated with IIoT deployments in the transportation sector. The maturity of risk management for organisations in the transport sector in SA is characterised by projects and is often reactive. Failure to manage risks effectively may result in the unavailability of IIoT devices and networks, damage to reputation, and possible compromise of trade secrets and sensitive information, as mentioned in Section 6.2.3.

6.4.3 IT Governance and Compliance

Robust IT governance frameworks and compliance mechanisms are required to ensure that IIoT deployments comply with regulatory requirements and industry standards in the transportation sector. Non-compliance with governance and compliance obligations may expose organisations to legal liabilities and regulatory sanctions (World Economic Forum, 2018). The governance processes for an IIoT environment in the transport sector of SA are characterised by projects and are often reactive. Reactive governance processes may overlook or delay the implementation of necessary security measures, leaving IIoT deployments vulnerable to cyber threats and attacks. This could lead to data breaches, operational disruptions, and compromised safety within the transportation infrastructure, as discussed in Section 6.2.1. Without solid governance mechanisms to ensure IIoT deployments comply with regulatory requirements, they could result in penalties, fines, or legal action, which are further discussed in Section 6.4.5.

6.4.4 Policies, Standards, and Procedures

Clear and comprehensive cybersecurity policies, standards, and procedures provide guidance and direction for employees and stakeholders involved in IIoT initiatives in the transportation sector. Inadequate or outdated policies may leave organisations vulnerable to security breaches and compliance violations (World Economic Forum, 2018).

Well-defined policies, standards, and procedures facilitate consistent and effective implementation of cybersecurity controls, promoting a culture of security awareness, accountability, and compliance across the organisation (Szuba, 1998).

6.4.5 Legal and Regulatory Requirements

Compliance with legal and regulatory requirements is essential for ensuring the legality, integrity, and security of IIoT deployments in the transportation sector. Failure to comply with applicable laws and regulations may result in legal consequences, fines, and penalties for organisations.

Understanding and adhering to legal and regulatory requirements help organisations navigate complex legal landscapes, mitigate legal risks, and uphold the rights and privacy of stakeholders and customers in South Africa’s transportation sector (Kianpour & Raza, 2024). Non-compliance with regulatory requirements could result in penalties, fines, or legal action against organisations operating within the transport sector. An example is a data breach where a transport company failed to take appropriate measures to protect personal information, resulting in a fine by the Information Regulator of South Africa (Moyo, 2023).

6.5 Research Objective 4 – To critically assess the People Factors Influencing IIoT Cybersecurity in the South African Transport Sector

This objective aimed to assess the people factors (cybersecurity awareness, enablement, employee engagement and employee satisfaction) influencing IIoT cybersecurity in the SA transport sector. Results from the quantitative data (questionnaire) analysis and document analysis are discussed in the section below.

Four people factors influence IIoT cybersecurity in the SA transport sector. They are cybersecurity awareness, enablement, employee engagement and employee satisfaction.

From the analysis in Section 4.6, it's crucial to note that while the general cybersecurity awareness in the South African transport sector is more mature, the specific awareness for IIoT cybersecurity is below managed. This indicates a reactive and project-based approach, highlighting the need for organisations to address the risk of IIoT awareness sufficiently. The importance of IIoT cybersecurity in the SA transport sector cannot be overstated.

The general security skills in an IIoT environment in the transport sector of SA are managed, but the maturity of the organisation enabling staff for general security skills is below managed. This underscores the significant role of employees in enhancing security measures. By empowering them, organisations can bridge the gap in general security skills.

The maturity of employees that have IIoT security skills in an IIoT environment in the transport sector of SA is even less mature between initial and managed, indicating the process is unpredictable, poorly controlled, and reactive. This situation underscores the urgent need for organisations to invest in training their employees to effectively manage IIoT security. The gap in IIoT security skills is even more pronounced, yet organisations fail to bridge this gap by adequately empowering their staff. Immediate action is needed to address this issue.

The maturity of the following engagements, which refer to the level of interaction and involvement, is all below managed and indicates a general lack of employee engagement with security staff in the transport sector of SA on all levels:

- Engineering/OT engagement with security staff.
- IT engagement with security staff.
- Management engagement with security staff and
- Executive management engagement with security staff.

The maturity of employee satisfaction within an organisation having an IIoT environment in the transportation sector of SA is below managed, which could be related to the organisation's failure to

provide tools to manage IIoT security and influence the employees' energy and productivity, as both these are also below managed.

The document analysis in Section 5.6 notes the main phrases or prevalent words from the IIoT documents. These demonstrate basic security principles applied to IIoT and will guide the development of the control framework in Section 6.7.3. The main phrases or prevalent words for each factor are displayed in Figure 6.7.

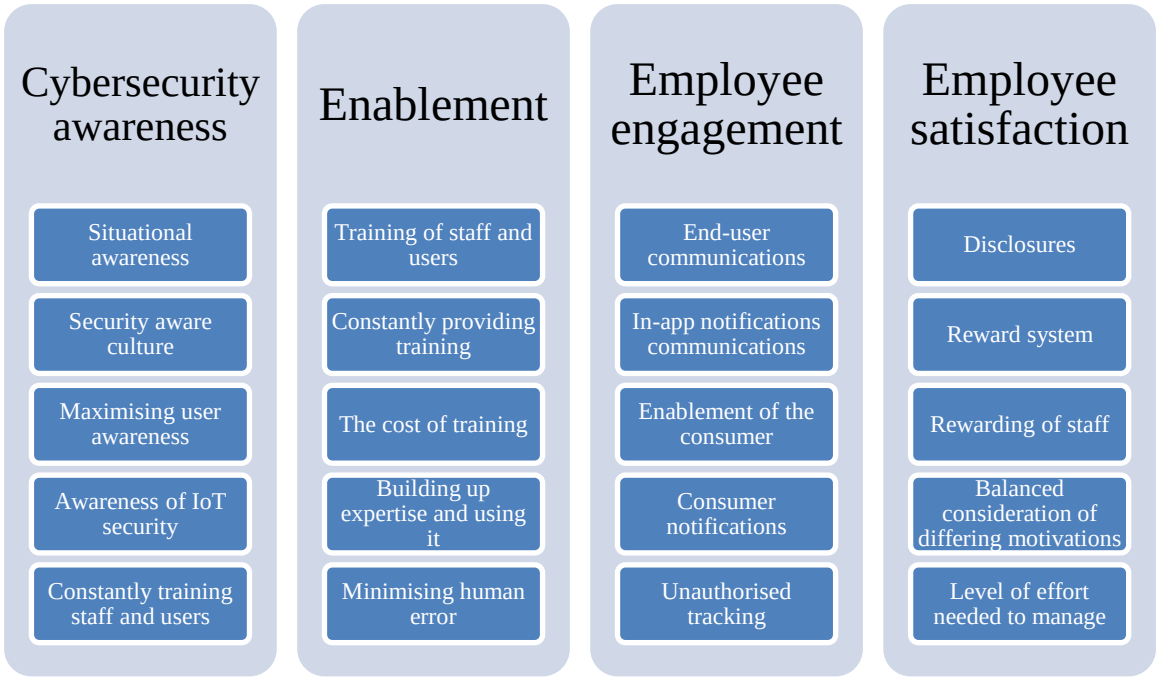


Figure 6-7: Main phrases for people factors

The factors above have the following impact on the transportation sector of South Africa as discussed in Section 6.5.1 – Section 6.5.4.

6.5.1 Cybersecurity Awareness

A lack of cybersecurity awareness among employees increases the likelihood of human errors, such as falling victim to phishing attacks or inadvertently disclosing sensitive information (Uchendu et al., 2021), which can compromise the security of IIoT systems in the transportation sector.

Investing in cybersecurity awareness training programs educates employees about the risks and best practices associated with IIoT cybersecurity. This empowers them to recognise and respond effectively to potential threats, reducing the organisation's overall risk exposure, as discussed in Section 6.4.1.

As discussed in Section 6.3.5, a strong security culture promotes cybersecurity awareness, accountability, and best practices among employees at all levels of the organisation. An immature security culture may result in a need for more awareness and understanding of cybersecurity risks

among employees in the transport sector. This can lead to careless activities, such as weak password management, failure to patch, and exposure to social engineering attacks, increasing the organisation's vulnerability to cyberattacks targeting IIoT systems.

6.5.2 Enablement

Insufficient resources, tools, and support hinder employees' ability to implement adequate cybersecurity measures and respond to security incidents in IIoT environments within the transportation sector. As discussed above, although there is a gap in general security skills in the transport sector of South Africa, the gap in IIoT security skills is even more significant. Without adequate enablement, employees may struggle in IIoT environments, including sensitive data from cyber threats (Hoffman, 2019); the organisations in the transport sector failed to bridge this gap by adequately empowering their staff. They should provide their employees with the necessary resources, training, and support to proactively identify and address cybersecurity challenges, fostering a culture of security and resilience within the organisation, as discussed in Section 6.3.5.

6.5.3 Employee Engagement

Low levels of employee engagement in cybersecurity initiatives result in decreased motivation, participation, and commitment to cybersecurity practices and protocols (Reeves, Delfabbro, & Calic, 2021). Disengaged employees may need to pay more attention to security policies and their responsibilities, exposing IIoT systems to potential vulnerabilities (Hoffman, 2019).

It is crucial to foster more employee engagement with security staff in the transport sector of SA on all levels, from engineering staff, OT staff, IT staff, management, and executive management. By promoting employee engagement through collaboration, communication, and recognition, we can encourage active participation in cybersecurity efforts. This, in turn, enhances the organisation's ability to address emerging threats and protect critical assets in the transportation sector (Reeves et al., 2021).

6.5.4 Employee Satisfaction

Employee dissatisfaction poses significant risks in cybersecurity. Dissatisfied employees are more likely to engage in risky behaviours, such as circumventing security protocols or neglecting security updates, which can compromise the integrity and security of IIoT systems. Moreover, low employee satisfaction can increase turnover rates, thereby exacerbating cybersecurity challenges (Adetoye & Fong, 2023).

The employees in an IIoT environment in the transport sector of SA are not satisfied. The organisation's failure to provide tools to manage IIoT security and influence the employee's energy and productivity could be a cause of this. Organisations must foster a positive work environment, providing tools and opportunities for professional development and recognising employees'

contributions to enhance job satisfaction, energy, and morale, promoting a culture of security and accountability as discussed in Section 6.3.5.

6.6 Research Objective 5 – To assess the Degree of the Relationships Amongst the BMIS Factors for IIoT Cybersecurity in the South African Transport Sector

The correlation between technological, organisational, procedural, and people factors is calculated to assess the degree of the relationships among the BMIS factors for IIoT cybersecurity in the SA transport sector.

The factors and their relationships are as follows: Architecture for the relationship between technological and organisational factors, enabling & support for technological and procedural factors, Human factors for technological and people factors, governing for organisational and procedural factors, culture for organisational and people factors, and Emergence for procedural and people factors. Visualisation hereof is shown in Figure 6-34.

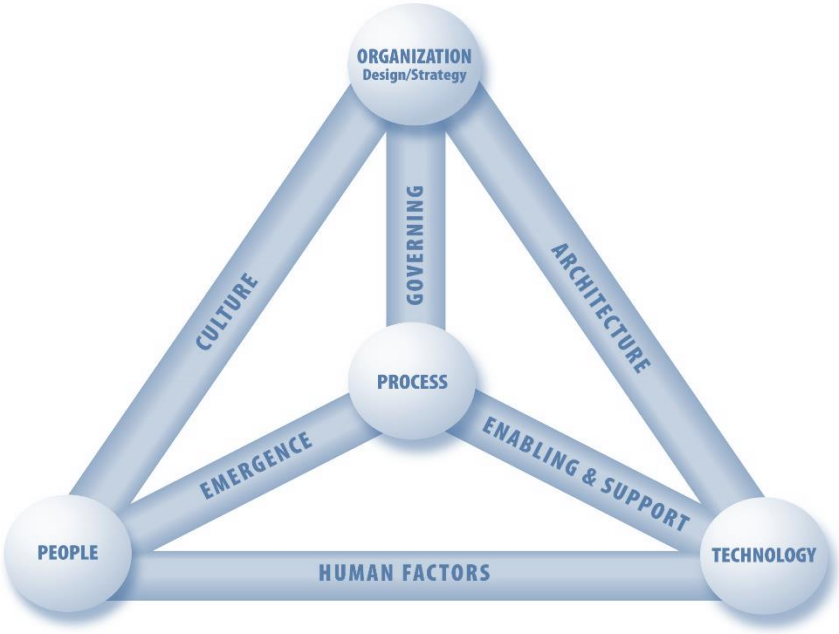


Figure 6-8: Business Model for Information Security (BMIS)

Source: ISACA (2010a: 13)

6.6.1 Relationship between Technological and Organisational Factors

6.6.1.1 Relationship between Technological (threats) and Organisational Factors

From the analysis in Section 4.7.1, it is observed that there are two strong correlations between one of the technological (threat) and organisational factors. A strong negative correlation exists between Denial-of-sleep and risk appetite for IIoT and a strong negative correlation between signal jamming attacks and governance processes for IIoT.

Six moderate negative correlations exist between the technological (threat) and organisational factors. These are displayed in Figure 6.9 and Figure 6.10 and discussed in Table 6.2. The two strong negative correlations are highlighted in a different colour.

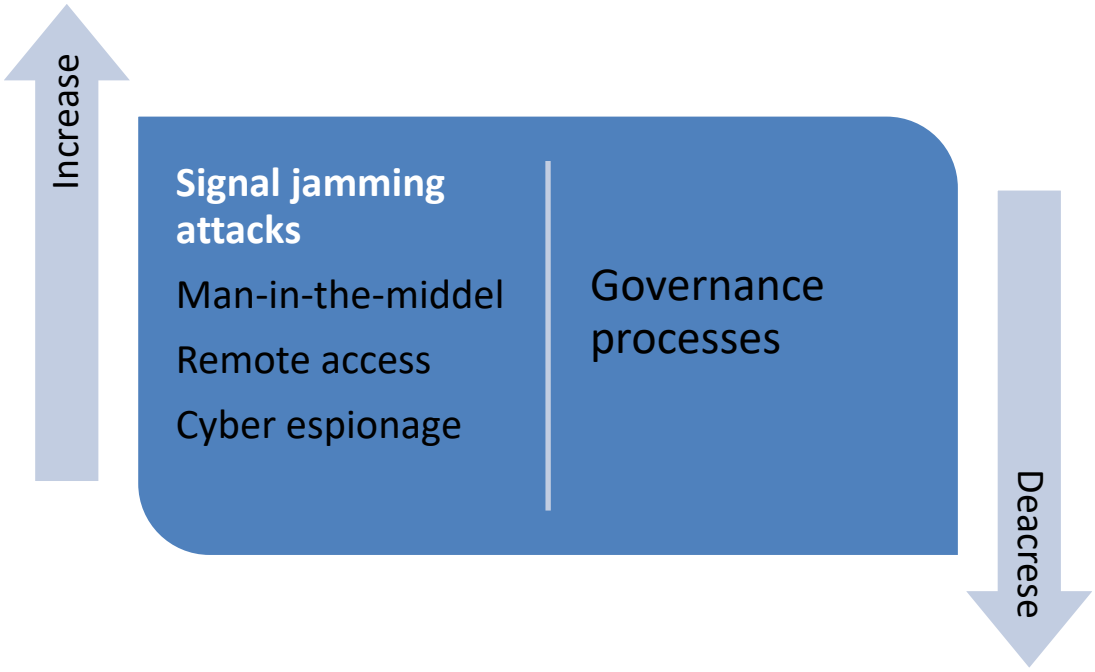


Figure 6-9: Negative correlation between technology (threats) and governance processes

Signal jamming attacks and governance processes for IIoT

- In the transport sector, IIoT plays a crucial role in Intelligent Transportation Systems (ITS) (Y. Wu et al., 2022). Governance processes ensure secure and efficient data communication between vehicles, infrastructure, and traffic management systems. A negative correlation could indicate that as governance processes weaken, the risk of signal jamming attacks disrupting communication within ITS increases, resulting in the unavailability of IIoT devices or networks, as discussed in Section 6.2.3
- Many transportation systems rely on GPS and other navigation technologies that are part of IIoT. A negative correlation may imply that as governance processes in the transport sector become less effective, the reliability of navigation systems decreases due to a higher risk of

signal jamming attacks affecting GPS signals. Recently, there were suspicions that Russia may have intentionally disrupted GPS signals on an aircraft transporting Grant Shapps, a British politician, prompting concerns about potential security implications. The incident underscores tensions and suspicions regarding Russia's involvement in cyber activities with potential international ramifications (The Guardian, 2024).

- Autonomous vehicles heavily depend on IIoT technologies for communication and decision-making (Biswas & Wang, 2023). Weak governance processes could expose these vehicles to signal jamming attacks, jeopardising their ability to navigate safely. The negative correlation may suggest that as governance processes decline, the security of autonomous vehicles against signal jamming diminishes.
- As discussed in Section 1.4, the transport sector is closely linked to supply chain logistics. Weakened governance processes may result in vulnerabilities within the supply chain's IIoT components, making it more susceptible to signal jamming attacks. The negative correlation could highlight the potential disruption to transportation-related supply chains when governance is inadequate.

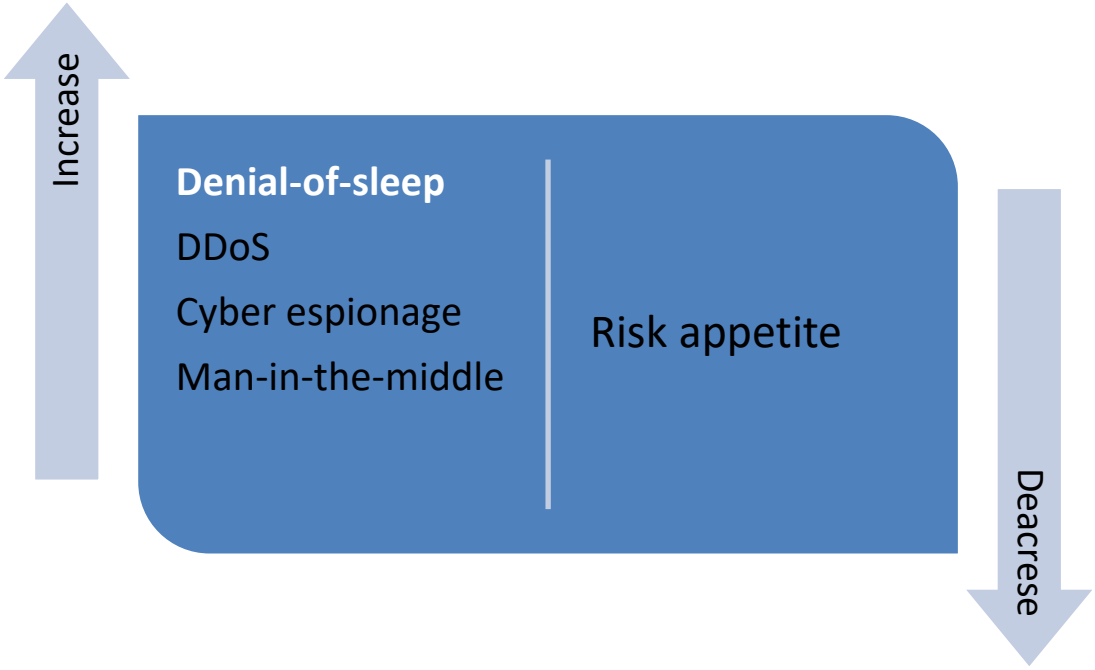


Figure 6-10: Negative correlation between technology (threats) and risk appetite

The two strong correlations above have the following impact on the transportation sector:

Denial-of-sleep vs risk appetite

- In the transport sector, where safety and reliability are paramount, organisations typically have low-risk appetites concerning disruptions or vulnerabilities that could endanger lives, cause

accidents, or disrupt transportation services. The strong negative correlation suggests that as the frequency or severity of Denial-of-sleep attacks increases, the willingness or tolerance for risk decreases. Based on the discussions in Section 6.4.2, the risk assessments and risk tolerance within an organisation with an IIoT environment in the transportation sector of SA still need to be fully developed and conducted comprehensively. It could suggest that risk assessments should be given more importance or deemed irrelevant once a threat has already materialised.

- Denial-of-sleep attacks targeting critical transportation systems can pose significant safety risks. For example, if traffic lights are disrupted, it could lead to accidents or traffic congestion, jeopardising public safety, as seen in the Polish tram incident in Section 2.3.7.1.2. Transport systems rely heavily on IIoT devices for efficient operations (Biswas & Wang, 2023). Denial-of-sleep attacks can disrupt these systems, leading to increased disruptions and safety concerns, as mentioned in Section 6.2.3.

The factors with a moderate correlation are listed in Table 6.2.

Table 6-2: Moderate correlations between technological factors and organisational factors

Technological factor	Organisational factor	Impact
DDoS (Moderate correlation)	Risk appetite	• The Potential consequences of DDoS attacks on IIoT systems are severe. These attacks can overwhelm the systems with a flood of traffic, disrupting their normal operation. A moderate negative correlation suggests that the risk appetite for IIoT decreases, and the susceptibility to DDoS attacks diminishes. In the transport sector, a lower risk appetite may prompt organisations to invest in robust DDoS mitigation strategies, ensuring the uninterrupted operation of critical transportation infrastructure and services.
Cyber espionage (Moderate correlation)		• A lower risk appetite for IIoT is linked to reduced susceptibility to cyber espionage activities. Organisations with a lower risk appetite in the transport sector may prioritise investments in cybersecurity measures, such as intrusion detection systems and encryption protocols, to safeguard against espionage threats targeting sensitive transportation data. The threat of cyber espionage and the risks associated with it are discussed in Section 6.2.1 and Section 6.2.3.
Man-in-the-middle (Moderate correlation)		• A lower risk appetite for IIoT is associated with decreased vulnerability to MitM attacks. In the transport sector, organisations with a lower risk appetite may implement stringent security measures, such as end-to-end encryption and certificate-based authentication, to mitigate the risk of unauthorised interception and manipulation of communication as Man-in-the-Middle attacks may lead to underestimation of security vulnerabilities, exposing transportation systems to potential disruptions and safety hazards as discussed in Section 6.2.3.
Man-in-the-middle (Moderate correlation)	Governance processes for IIoT	• As the susceptibility to Man-in-the-Middle attacks increases, the effectiveness of governance processes decreases. In the transport sector, this correlation indicates that vulnerabilities in governance processes may exacerbate the risk of Man-in-the-Middle attacks compromising critical communication networks, leading to potential disruptions in traffic management and safety systems.

Technological factor	Organisational factor	Impact
Remote access (Moderate correlation)		• As remote access vulnerabilities in IIoT systems increase, the strength of governance processes diminishes. In the transport sector, inadequate governance processes may exacerbate the risk associated with unauthorised remote access, potentially leading to security breaches in control systems, such as such as railway signalling systems or traffic lights, which could cause accidents or congestion.
Cyber espionage (Moderate correlation		• As the risk of cyber espionage targeting IIoT systems rises, the effectiveness of governance processes declines. In the transport sector, compromised governance processes may result in inadequate protection of sensitive data and infrastructure, increasing the likelihood of cyber espionage targeting transportation networks and critical infrastructure, as discussed in Section 6.2.1.

6.6.1.2 Relationship between Technological (vulnerabilities) and Organisational Factors

It is observed from the analysis in Section 4.7.1 that there is no strong correlation between any of the technological (Vulnerabilities) and organisational factors. There is only one moderate correlation between insecure default settings and employees supporting IIoT. Insecure default settings on IIoT devices create potential entry points for cyberattackers. If employees supporting IIoT devices are not sufficiently trained, as discussed in Section 6.5.2, it increases the risk of unauthorised access or exploitation of vulnerabilities by malicious actors. This could lead to data breaches, system compromises, or disruption of operations due to the unavailability of IIoT devices or networks.

Insecure default settings in IIoT devices used for safety-critical functions in the transport sector, such as traffic management or vehicle monitoring systems, pose significant risks. Employees who need more knowledge or training to address these security flaws may inadvertently compromise safety measures. This could lead to the risk of human safety discussed in Section 6.2.3, such as accidents, injuries, or even loss of life due to malfunctions or manipulations of critical transportation systems.

This highlights the importance of implementing comprehensive cybersecurity training programs, establishing clear security policies, and conducting regular audits to ensure IIoT devices are configured securely. By empowering employees with the knowledge and tools to address security risks effectively, organisations can enhance the resilience of their industrial systems and mitigate the potential impact of cyber threats.

6.6.1.3 Relationship between Technological (risks) and Organisational Factors

From the analysis in Section 4.7.1, it is also observed that there is no strong or moderate correlation between any of the technological (Risks) and organisational factors. It suggests that vulnerabilities or risks alone may not strongly influence organisational factors in the context of analysis.

6.6.2 Relationship between Technological and Procedural Factors

6.6.2.1 Relationship between Technological (threats) and Procedural Factors

Section 4.7.2 observes only one strong correlation between the technological (threat) and procedural factors: a strong negative correlation between Denial-of-sleep and risk assessment for IIoT. Some moderate negative correlations exist between the technological (threat) and procedural factors. These are displayed in Figure 6.11 and discussed in Table 6.3.

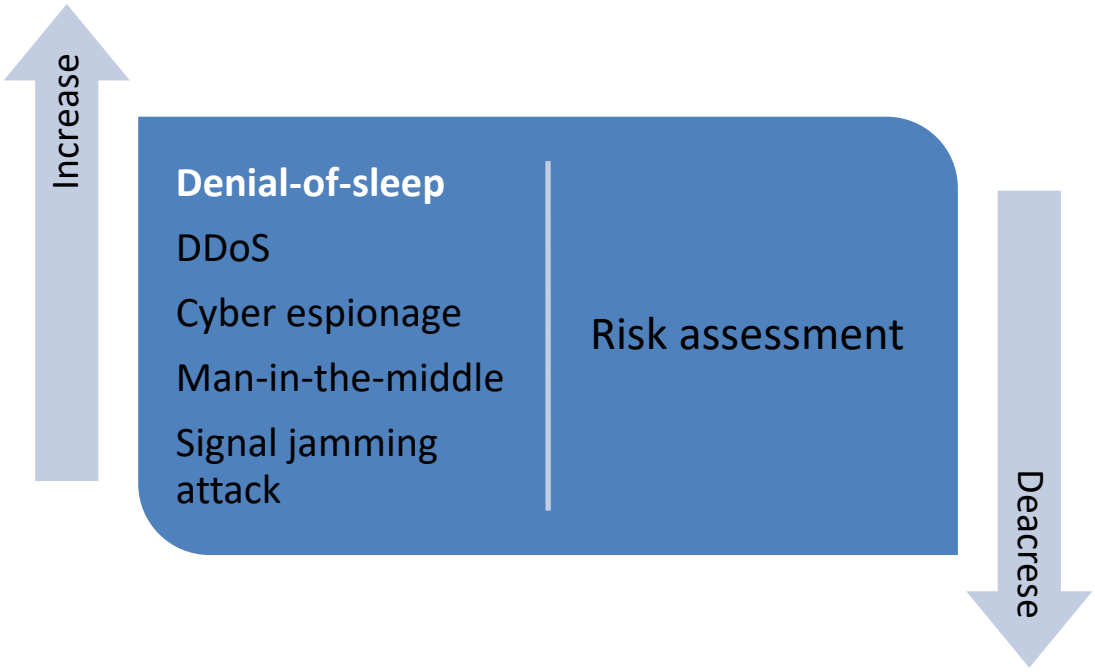


Figure 6-11: Negative correlation between technology (threats) and procedural factors

Denial-of-sleep vs risk assessments

- The strong negative correlation between the technological factor, Denial-of-sleep (a threat related to disrupting IIoT device functionality) and the organisational factor, as the frequency or severity of Denial-of-sleep attacks increases, the willingness to conduct risk assessments decreases. Organisations may be less likely to conduct comprehensive risk assessments when facing significant threats like Denial-of-sleep. Based on the discussions in section 6.4.2, the risk assessments and risk tolerance within an organisation with an IIoT environment in the transportation sector of SA still need to be fully developed and conducted comprehensively. It could suggest that either risk assessments are not given enough importance or are deemed irrelevant once a threat has already materialised.
- A negative correlation could also imply that as the frequency of these attacks increases, the reliability of transport systems decreases. With an accurate risk assessment, transportation

authorities may allocate resources effectively to mitigate the impact of such attacks, leading to increased disruptions and safety concerns, as mentioned in Section 6.2.3.

The factors with a moderate correlation are listed in Table 6.3.

Table 6-3: Moderate correlation between technological (threat) and procedural factors

Technological factor (threat)	Procedural factor	Impact
DDoS	Risk assessment	• This indicates that as the occurrence or severity of DDoS attacks increases, the level of risk assessment for IIoT tends to decrease, and the effectiveness of risk management for IIoT tends to decrease. It implies that organisations with a higher prevalence of DDoS attacks might encounter difficulties conducting thorough risk management activities for IIoT systems. DDoS attacks can disrupt transport systems, causing delays, cancellations, or inefficiencies in public transportation or freight logistics.
Cyber espionage		• As the risk of cyber espionage rises, the extent of risk assessment for IIoT tends to decrease. Organisations may focus more on preventing or addressing espionage incidents than conducting comprehensive risk assessments.
Man-in-the-middle		• As the risk of Man-in-the-Middle attacks increases, the accuracy of risk assessments decreases. In the transport sector, compromised risk assessment processes due to Man-in-the-Middle attacks may lead to underestimation of security vulnerabilities, exposing transportation systems to potential disruptions and safety hazards, as discussed in Section 6.2.3.
Signal jamming attack		• As the occurrence or threat of signal jamming attacks increases, the effectiveness of risk assessment for IIoT tends to decrease. It suggests that organisations encountering a higher prevalence of signal jamming attacks may have difficulty performing comprehensive risk assessments specifically for IIoT security. In the transport sector, a negative correlation could indicate that as risk assessments weaken, the risk of signal jamming attacks disrupting communication within transport systems increases.

6.6.2.2 Relationship between Technological (vulnerabilities) and Procedural Factors

From Section 4.7.2, it is observed that there is no strong correlation between the technological (vulnerabilities) and procedural factors. There are some moderate correlations between the two factors. These are displayed in Table 6.4.

Table 6-4: Moderate correlation between technological (vulnerabilities) and procedural factors

Technological factor (vulnerabilities)	Procedural factor	Impact
Use of insecure or outdated components	Organisation has an incident response plan	• Organisations that utilise insecure or outdated components are more likely to have an incident response plan. It suggests that despite using vulnerable components, these organisations have taken measures to prepare for potential security incidents
No privacy protection		• There is a moderate positive correlation between no privacy protection and an organisation that has an incident response plan, which indicates that organisations that lack privacy protection measures tend to also have an incident response plan in place.

Technological factor (vulnerabilities)	Procedural factor	Impact
		While privacy protection may be lacking, organisations still recognise the importance of planning to respond to security incidents.
Insecure Network Services		• Organisations with insecure network services are more likely to have incident response plans. In the transport sector, where secure and reliable data communication is crucial for operational efficiency and passenger safety (Koroniotis, Moustafa, Schiliro, Gauravaram, & Janicke, 2020), the recognition of vulnerabilities in network services and data handling processes prompts organisations to develop incident response plans to address potential breaches and minimise the impact on operations.
Insecure Data Transfer and Storage		• Organisations with data transfer/storage practices are more likely to have incident response plans. This would have a similar impact as the insecure network services discussed above.
Misconfiguration (negative)	Governance processes for IIoT	• As the prevalence of misconfigurations decreases, the effectiveness of governance processes for IIoT increases. Misconfigurations in IIoT devices and systems can introduce vulnerabilities and weaken overall governance and control mechanisms. • In the transport sector, where integrating IIoT technologies is pervasive (Madakam & Uchiya, 2019), reducing misconfigurations enhances the resilience of governance processes and control frameworks, mitigating the risk of security incidents and operational disruptions.
	Control framework for IIoT	• As misconfigurations become more prevalent, the maturity of the control framework for IIoT tends to decrease. It suggests that organisations experiencing misconfigurations may have difficulties establishing a mature control framework for IIoT security. This aligns with the discussion in Section 6.4.4 on the maturity of policies, procedures, frameworks, and standards for IIoT.

6.6.2.3 Relationship between Technological (risk) and Procedural Factors

From Section 4.7.2, it is noted that there is no strong correlation between any of the technological (risk) and procedural factors.

There is one moderate negative correlation between physical asset damage and IIoT security policies/procedures/controls implemented. This suggests that as the potential for physical asset damage increases, the implementation of security policies, procedures, and controls specifically designed for IIoT decreases. This implies that organisations facing a higher risk of physical asset damage due to IIoT vulnerabilities may have inadequate security measures. These organisations may not prioritise or adequately address developing and implementing security policies, procedures, and controls essential for protecting IIoT systems. The potential for physical asset damage can have significant consequences, including operational disruptions and safety concerns as mentioned in Section 6.2.3. This correlation highlights the importance of SA transport sector organisations to strengthen their security posture by implementing robust security policies, procedures, and controls tailored explicitly for IIoT environments.

6.6.3 Relationship between Technological and People Factors

6.6.3.1 Relationship between Technological (threats) and People Factors

From Section 4.7.3, it is observed that there is no strong or moderate correlation between any of the technological (threat) and people factors.

6.6.3.2 Relationship between Technological (vulnerabilities) and People Factors

From Section 4.7.3, it is observed that there is no strong correlation between any of the technological (vulnerabilities) and people factors.

There are, however, also some moderate negative correlations between the technological (vulnerabilities) and people factors. These are displayed in Figure 6.12 and Figure 6.13 and discussed in Table 6.5.

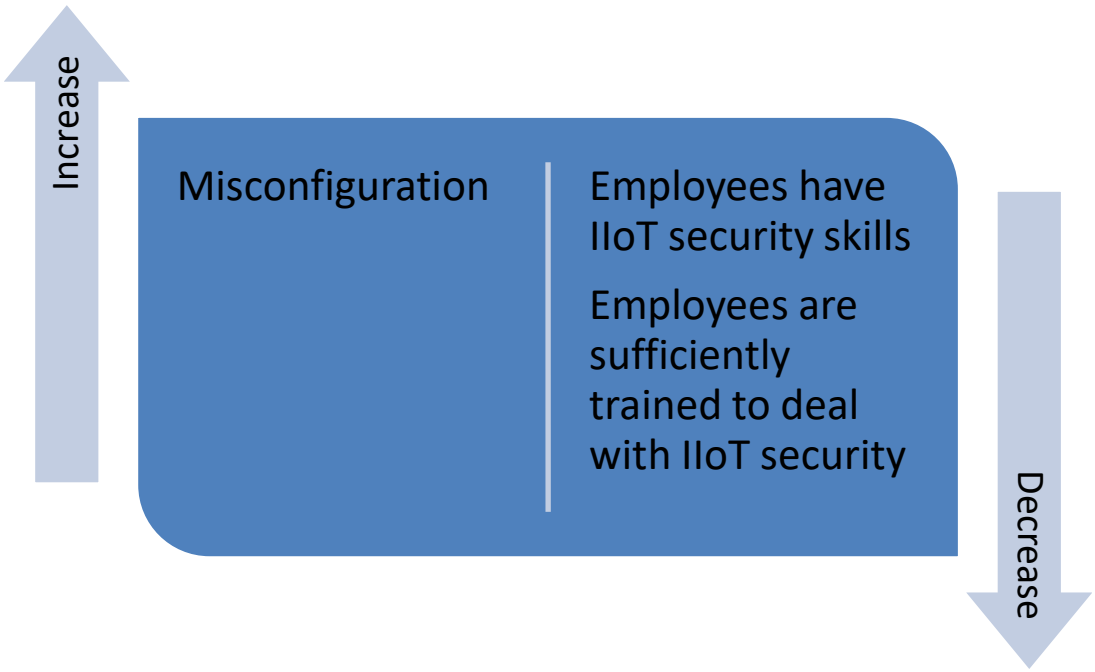


Figure 6-12: Negative correlation between misconfiguration and people factors

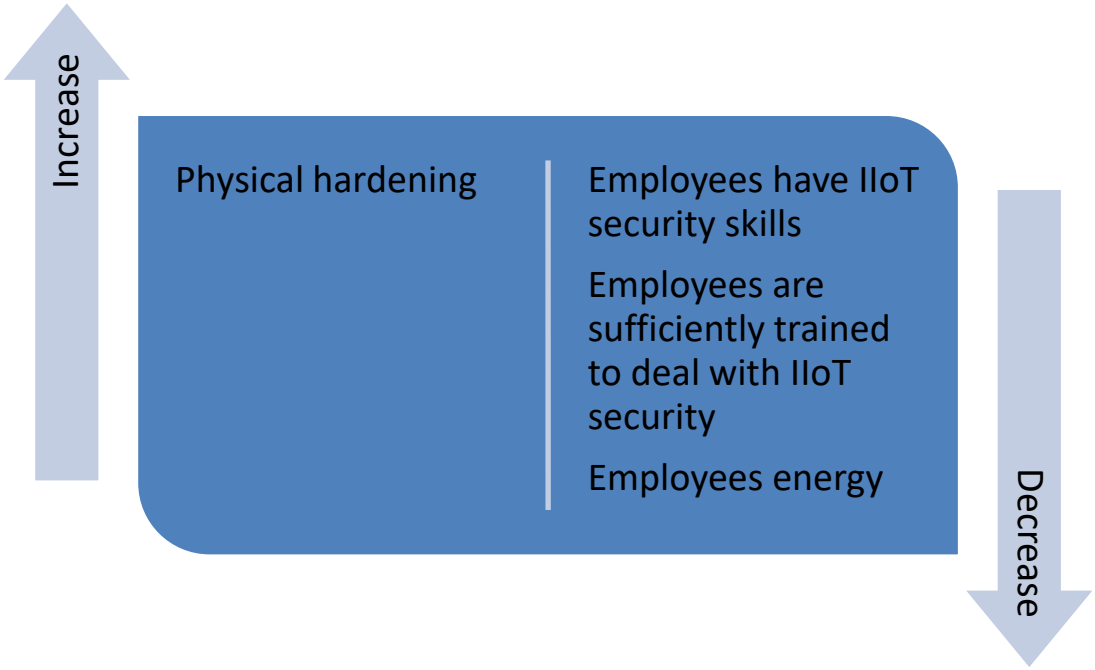


Figure 6-13: Negative correlation between physical hardening and people factors

The factors with a moderate correlation are listed in Table 6.5.

Table 6-5: Moderate correlation between technological (vulnerabilities) and people factors

Technological factor (vulnerabilities)	**People factor**	**Impact**
Misconfiguration	Employees have IIoT security skills Employees are sufficiently trained to deal with IIoT security	• As misconfigurations in IIoT systems increase, the level of security skills and employee training decreases. • In the transport sector, where the integration of IIoT technologies is extensive (Y. Wu et al., 2022), misconfigurations can pose significant security risks, such as disruptions to traffic management systems or compromises to vehicle safety. • The negative correlations indicate a potential gap in employee knowledge and preparedness to address these vulnerabilities effectively, which can increase the likelihood and impact of security incidents.
Physical Hardening	Employees have IIoT security skills Employees are sufficiently trained to deal with IIoT security	• It's important to note that inadequate physical security measures not only pose direct risks but also indirectly contribute to a decrease in employee readiness to handle IIoT security challenges. This underscores the need for comprehensive security measures. • In the transport sector, where physical infrastructure plays a crucial role in ensuring the reliability and safety of transportation systems (Mohebbi et al., 2020), the absence of physical hardening can expose critical components to risks such as vandalism, tampering, or unauthorised access as seen in Section 2.3.7.1. • Employees may lack the skills and training to address these physical security vulnerabilities effectively, leaving

Technological factor (vulnerabilities)	People factor	Impact
		transportation systems vulnerable to exploitation by malicious actors.
	Employees energy	• As the lack of physical hardening increases, employees' energy levels decrease. While the direct impact of employee energy levels on security vulnerabilities may not be immediately apparent, it could indirectly affect their ability to effectively detect, respond to, and mitigate security threats. • In the transport sector, where operational efficiency and responsiveness are essential for maintaining smooth transportation services (Hindarto, 2023), employee fatigue or decreased energy levels could impair their capacity to address security incidents promptly, potentially leading to prolonged disruptions or compromises to passenger safety as discussed in the risks in Section 6.2.3.

These correlations highlight the importance of investing in employee training and awareness programs to enhance security skills and preparedness in the transport sector. By equipping employees with the necessary knowledge and capabilities to identify and mitigate security vulnerabilities, organisations can bolster the resilience of transportation systems against cyber threats.

6.6.3.3 Relationship between Technological (risk) and People Factors

From Section 4.7.3, it is noted that there are no strong or moderate correlations between any of the technological (risk) and people factors. This means the relationship between these two sets of factors is not significant or notable based on the observed correlation coefficients. The lack of strong or moderate correlations indicates that changes in the technological (risk) factors are not strongly associated with corresponding changes in the people factors. This means that variations in technological risks do not significantly impact the skills, awareness, or engagement levels of the individuals involved in IIoT cybersecurity.

6.6.4 Relationship between Organisational and Procedural Factors

From Section 4.7.4, it is observed that there are strong correlations between the organisational and procedural factors. The top five are listed and discussed in Table 6.5 below.

Table 6-6: Strong correlation between organisational and procedural factors

Organisational factor	Procedural factor	Impact
Cybersecurity roadmap/strategy supporting IIoT	Risk assessment for IIoT	• Organisations with a well-defined cybersecurity roadmap or strategy that supports IIoT are more likely to conduct comprehensive risk management for IIoT. • Transport systems rely heavily on IIoT devices for efficient operations (Biswas & Wang, 2023). Having a well-defined cybersecurity strategy aligned with IIoT objectives is crucial. A robust risk assessment process ensures that potential security threats and vulnerabilities, as discussed in Section 6.2.1 and Section 6.2.2, specific to IIoT deployments, are identified and

Organisational factor	Procedural factor	Impact
		mitigated effectively, enhancing the overall resilience of transportation systems.
Governance processes for IIoT		• An organisation with robust governance processes specific to IIoT are more likely to perform thorough risk management for IIoT. • As discussed in Section 6.6.1.1, governance processes ensure the secure and efficient communication of data between vehicles, infrastructure, and traffic management systems. Aligning governance processes with risk assessment activities enables organisations to systematically identify, evaluate, and address security risks associated with IIoT deployments, fostering a culture of security and resilience across transportation operations.
Innovative culture in the organisation		• Organisations fostering an innovative culture are more inclined to prioritise and conduct risk management for IIoT. • In the transport sector, where technological innovation drives advancements in traffic management, autonomous vehicles, and passenger services (Oladimeji et al., 2023), fostering an innovative culture encourages the adoption of cutting-edge IIoT solutions (Shah, Madni, Hashim, Ali, & Faheem, 2024). Incorporating risk assessment into the innovation process guarantees that potential security ramifications are addressed at the outset, allowing organisations to effectively balance innovation with strategies for mitigating risk.
Security culture in the organisation		• Organisations fostering an innovative culture are more inclined to prioritise and conduct risk management for IIoT. • In the transport sector, where technological innovation drives advancements in traffic management, autonomous vehicles, and passenger services (Oladimeji et al., 2023), fostering an innovative culture encourages the adoption of cutting-edge IIoT solutions (Shah et al., 2024). However, it's crucial to note that incorporating risk assessment into the innovation process is not just a formality, but a vital step that guarantees potential security ramifications are addressed at the outset, reassuring organisations about the safety of their IIoT implementations.
Senior / Executive understanding of IIoT security risks		• When senior executives better understand IIoT security risks, the organisation will likely conduct risk management for IIoT. • In the transportation sector, where strategic decision-making shapes the integration and execution of IIoT solutions, obtaining executive endorsement and backing for risk assessment endeavours is critical. This support is instrumental in fostering organisational resilience and guaranteeing the secure integration of IIoT technologies throughout transportation networks (Shah et al., 2024).

These strong correlations highlight the importance of organisational factors, such as cybersecurity strategy, governance processes, culture, and senior executive involvement, in driving the implementation of risk management practices for IIoT. They suggest that organisations with a proactive and security-conscious approach prioritise risk management activities and address the risks associated with IIoT more effectively.

6.6.5 Relationship between Organisational and People Factors

It is observed from Section 4.7.5 that there are three strong correlations between the organisational and people factors. They are displayed and discussed in Table 6.7.

Table 6-7: Strong correlation between organisational and people factors

Organisational factor	People factor	Impact
Security staff	IT engagement with security staff	• This suggests that when there is active engagement and collaboration between security staff and IT staff, the organisation is more likely to have a higher level of security awareness. • Organisations with dedicated cybersecurity staff are more likely to have active engagement between their IT teams and cybersecurity personnel. From Section 6.3, it is noted that there is a massive gap in the IIoT security staffing as most staff are allocated as part of a project and not dedicated to IIoT security. This aligns with the discussion in Section 6.5.3, where it was noted that there was a general lack of employee engagement with security staff in the transport sector of SA on all levels. • In the transport sector, where IIoT technologies are widely integrated, having dedicated cybersecurity staff is crucial for safeguarding critical infrastructure and passenger safety. Active engagement between IT and cybersecurity teams facilitates collaboration in identifying, assessing, and mitigating security risks associated with IIoT deployments. This collaboration ensures that cybersecurity considerations are integrated into IT operations, enhancing the overall security posture of transportation systems.
Risk assessment for IIoT	Security awareness specific for IIoT	• Organisations conducting thorough risk assessments for IIoT are more likely to have a higher level of security awareness specific to IIoT among their employees. • In the transport sector, where the reliance on IIoT devices and systems is pervasive (Madakam & Uchiya, 2019), understanding the distinctive cybersecurity challenges associated with these technologies is essential. Cybersecurity awareness training specific to IIoT equips employees with the knowledge and skills to recognise and mitigate security risks, enhancing the resilience of transportation systems against cyber threats.
Governance processes for IIoT		• Indicates that organisations with robust governance processes for IIoT are more likely to have a higher level of security awareness specific to IIoT among their employees. • Integrating cybersecurity awareness specific to IIoT into governance processes strengthens the governance framework for IIoT deployments in the transport sector. By incorporating security considerations into governance policies and procedures, organisations can ensure compliance with regulatory requirements, mitigate security risks, and foster a culture of security-conscious decision-making across transportation operations.

These correlations highlight the relationship between organisational factors, such as governance processes, senior executive involvement, and innovative culture, and the level of security awareness specific to IIoT among employees. They indicate that organisations that prioritise risk assessments, have effective governance processes, and promote engagement and collaboration between different

teams are likelier to foster a culture of security awareness and knowledge about IIoT security risks among their employees.

6.6.6 Relationship between Procedural and People Factors

From Section 4.7.4, it is noted that there are strong correlations between the procedural and people factors; they are displayed and discussed in Table 6.8.

Table 6-8: Strong correlation between procedural and people factors

Procedural factor	People factor	Impact
Control framework for IIoT	Employees are sufficiently trained to deal with IIoT security	• Organisations with a comprehensive control framework for IIoT are more likely to have adequately trained employees to handle IIoT security issues. • In the transport sector, where the deployment of IIoT technologies is widespread, e.g., traffic management systems and vehicle monitoring, as discussed in Section 2.4.7, having a robust control framework is essential for managing security risks effectively. By providing comprehensive employee training, organisations can enhance their ability to implement and adhere to security controls, reducing the likelihood of security breaches and operational disruptions.
Control framework for IIoT	Security awareness specific for IIoT	• Organisations with established governance processes for IIoT are more likely to prioritise cybersecurity awareness training tailored to these technologies. • Governance processes play a crucial role in defining policies, procedures (Tunny, n.d.), and oversight mechanisms for IIoT deployments in the transport sector. • Incorporating cybersecurity awareness that is specific to IIoT into governance processes can embed security considerations into decision-making frameworks and operational workflows. This proactive approach can enhance employee readiness to address security challenges associated with IIoT technologies, thus strengthening the overall security posture of transportation systems.
Governance processes for IIoT		• Organisations with solid governance processes for IIoT are likelier to have a higher level of security awareness specific to IIoT among their employees. • In the transport sector, where protecting critical infrastructure and passenger safety is paramount (Sammon & Caverly, 2007), aligning control frameworks with cybersecurity awareness initiatives enhances the resilience of transportation systems against cyber threats, as discussed in Section 6.2.1.
IIoT security policies/procedures/controls implemented	The organisation provides the tools to manage IIoT security	• Organisations implementing adequate security policies, procedures, and controls for IIoT are more likely to provide their employees with the necessary tools to manage IIoT security. • In the transport sector, the intricate and expansive nature of IIoT deployments presents significant security challenges (Jayalaxmi, Saha, Kumar, Kumar, & Kim, 2021). In this context, the importance of comprehensive policies, procedures, and controls for mitigating risks (Adaros Boye, Kearney, & Josephs, 2018) becomes even more pronounced. By providing the necessary

Procedural factor	People factor	Impact
		tools and resources for managing IIoT security, organisations can effectively enforce security measures, monitor for threats, and respond to incidents promptly, thereby bolstering the security of transportation systems.

These correlations highlight the importance of comprehensive control frameworks, robust governance processes, and implemented security policies, procedures, and controls in ensuring that employees are adequately trained, engaged, and equipped to handle IIoT security challenges. They indicate that organisations prioritising these factors are more likely to have a knowledgeable, trained, and prepared workforce to address IIoT security risks and effectively implement security measures.

6.7 Research Objective 6 – To Develop and Validate a Cybersecurity Framework for IIoT in the South African Transport Sector using the Data Collected

The conceptual framework is discussed in Section 3.3, and guidelines 1 and 3 for DSR of the Information Systems research framework from Hevner et al. (2004) are followed to develop and validate a cybersecurity framework for IIoT in the South African transport sector. Refer to Figure 6.14 for the conceptual framework with guidelines 1 and 3.

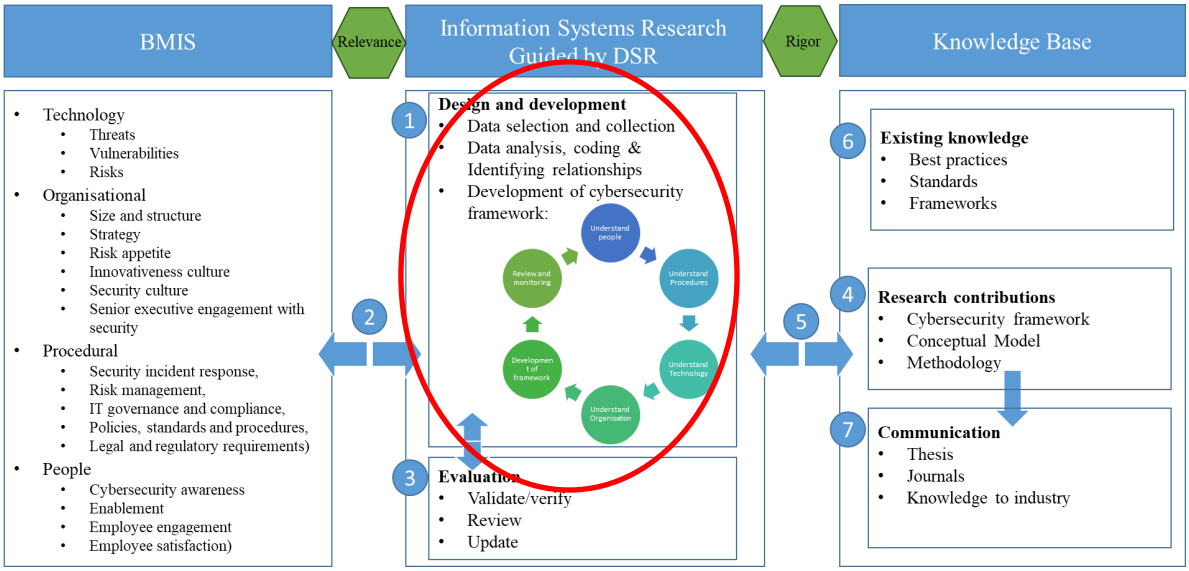


Figure 6-14: Conceptual Framework with guidelines 1 and 3 highlighted

Source: Author compiled

The following steps under design and development**,** guideline 1 (circled in red) are followed to conduct the case study, identify relationships, and develop a cybersecurity framework:

- Data selection and collection.
- Data analysis, coding and identifying relationships.
- Development of cybersecurity framework.
- Validate/verify and review.

6.7.1 Data Selection and Collection.

As discussed in Section 3.2.4, quantitative data (Questionnaires) were collected from participants in the transport sector with knowledge of IIoT and qualitative data were collected from best practices, standards, and frameworks selected in Section 5.2.1. These results are triangulated to determine the factors influencing cybersecurity for IIoT in the transport sector, as discussed in Sections 6.2 – 6.5. Outputs from these will guide the development of the cybersecurity framework.

6.7.2 Data Analysis, Coding, and Identifying Relationships

The data collected are analysed and coded, and relationships are identified in Sections 6.2 to 6.6. The Figure 6.15 below summarises the top results for each of the factors (Technological, Organisational, Procedural and People) used as input into the Research framework.

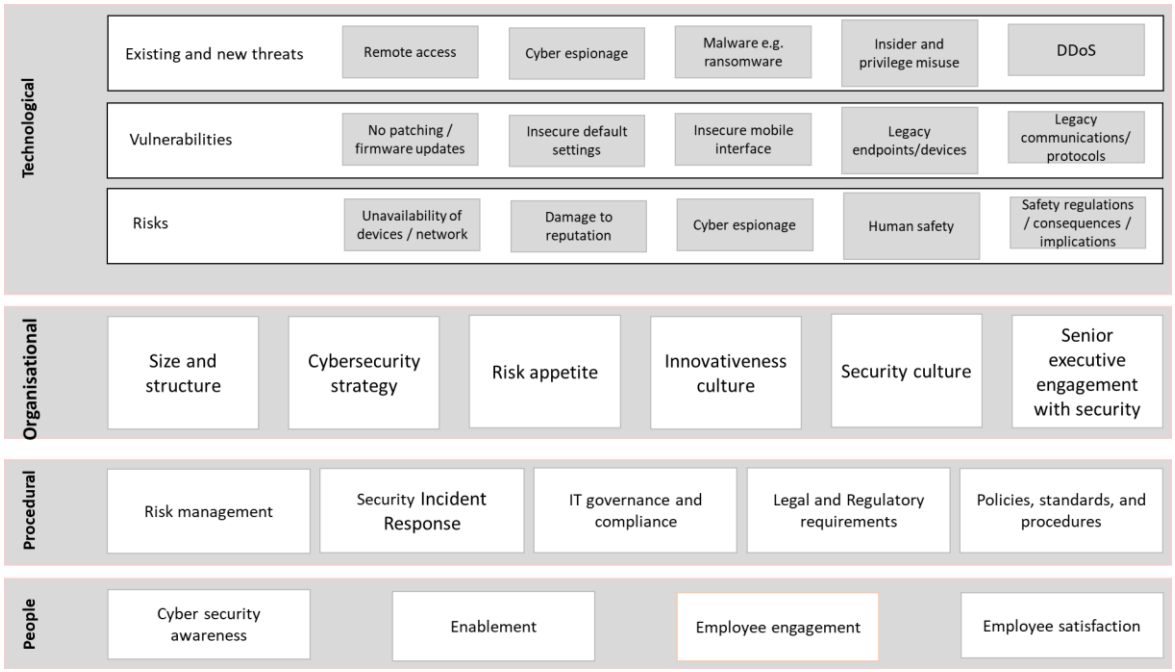


Figure 6-15: Summary of results

6.7.2.1 Maturity of Controls

It is noted from Section 4.5.7 that the top 3 responses for the maturity of controls to protect against the risk imposed by new IIoT are segmentation (firewall, standalone) with a mean of 2.80 (leaning towards defined – processes characterised for the organisation and is proactive), authentication or authorisation with a mean of 2.74, also leaning towards defined and combined third, secure protocols and regular and secure updates (patching) both with a mean of 2.66, which is between managed and defined.

Organisations within the transportation sector of SA have implemented specific processes and proactive measures to address the risks posed by new IIoT technologies. They have prioritised the implementation of segmentation controls, authentication and authorisation mechanisms, secure protocols, and regular updates. These measures aim to protect against the potential risks and vulnerabilities associated with IIoT. By implementing tailored processes and proactive measures, organisations in the transportation sector of SA are demonstrating their commitment to ensuring the security and protection of their IIoT systems and infrastructure.

The top five controls to protect against the risk imposed by new IIoT in the transportation sector of SA are:

- Segmentation (Firewall, standalone).
- Authentication and authorisation.
- Secure protocols.
- Regular and secure updates (patching) and
- Systems monitoring.

6.7.3 Development of Cybersecurity Framework

As discussed in Section 2.5, the process of developing a control framework is illustrated in Figure 6.16.

Figure 6-16: Framework Development Methodology

Adapted from: CPNI (2008)

Each of the framework development steps is discussed in Sections A to F.

A. Understand the People

Understand the people under this step; the organisation needs to assess the people element. The factors influencing the people aspect of an IIoT environment in the transportation sector of SA are determined, as discussed in Section 6.5, and populated in Section 6.7.2.4. This is used as input to develop the cybersecurity framework for an IIoT environment in the transportation sector of South Africa.

B. Understand the Process

Under this step, the organisation needs to assess the process element. The factors influencing the process aspect for an IIoT environment in the transportation sector of SA are determined, as discussed in Section 6.4, and populated in Section 6.7.2.3. This is used as input to develop the cybersecurity framework for an IIoT environment in the transportation sector of South Africa.

C. Understand the Technology

Under this step, the organisation needs to assess the technology element. The factors influencing the technology aspect of an IIoT environment in the transportation sector of SA are determined, as discussed in Section 6.2, and populated in Section 6.7.2.1. This is used as input to develop the cybersecurity framework for an IIoT environment in the transportation sector of South Africa.

D. Understand the Organisation

Under this step, the organisation needs to assess the organisational element. The factors influencing the organisational aspect of an IIoT environment in the transportation sector of SA are determined, as discussed in Section 6.3, and populated in Section 6.7.2.2. This is used as input to develop the cybersecurity framework for an IIoT environment in the transportation sector of South Africa.

E. Development of the Cybersecurity Framework

A cybersecurity framework is developed based on the business risk assessment and data collected, which include the people, procedural, technological and organisational factors of the IIoT environment in the transportation sector of South Africa. The high-level framework is listed in Table 6.9, with prevalent controls to implement guided by the key phrases identified as part of the document analysis on the security control frameworks listed in Section 5.2.1. These are based on technological, organisational, procedural and people factors influencing IIoT cybersecurity in the SA transport sector, as discussed in Section 6.7.2. The time frame for implementation is listed below in Figure 6.17, with five phases adapted Subramanian (2023) and based on NIST (National Institute of Standards and Technology, 2019) and COBIT (ISACA, 2018) control framework implementation. The details of each control are discussed in Section 6.7.3.1 to Section 6.7.3.29.

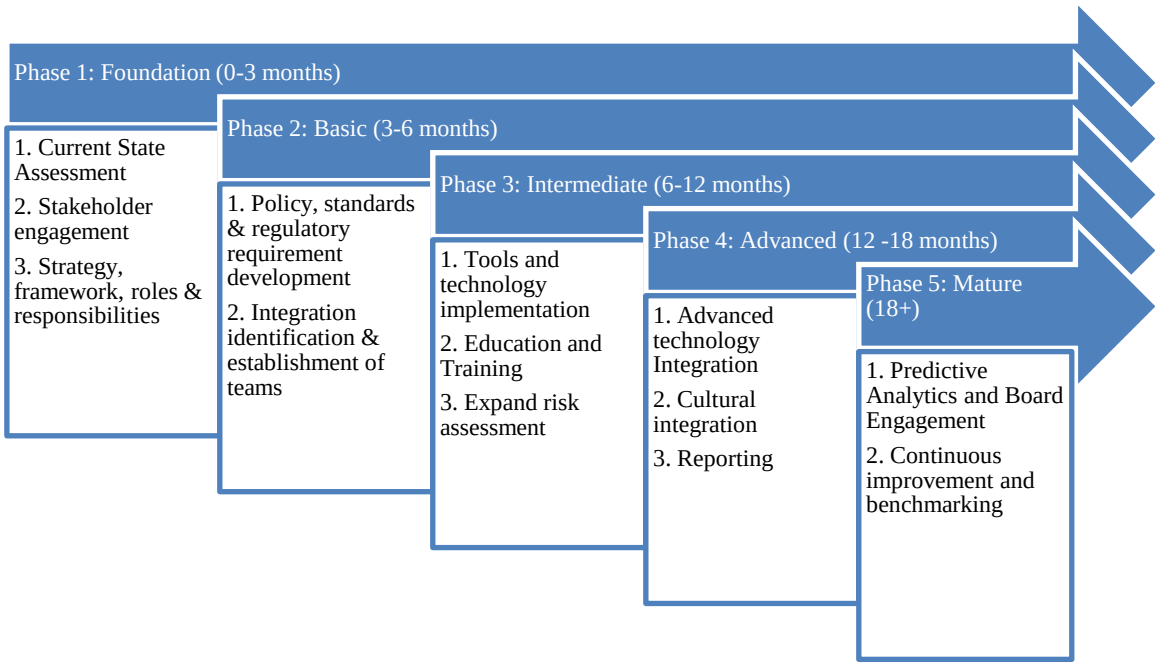


Figure 6-17: Control implementation phases

Adapted from: Subramanian (2023)

F. Validate / Verify and Review

A regular review of the IIoT environment in the transportation sector of SA needs to take place to identify new threats, vulnerabilities, and risks, and the corresponding updates of the cybersecurity framework should take place at a minimum of annually (CPNI, 2008; Minett, 2022) or more frequent depending on the risk profile of the organisation (NIST, 2019; ISACA, 2018) in line with industry best practices.

Table 6-9: Cybersecurity Framework with IIoT controls

Control	Reference	Justification	Threat / Vulnerability / Risk	Phase
Risk Management	Section 6.7.3.1	Top organisational & Procedural	Immaturity of the risk appetite	1 & 3
Executive Engagement Program	Section 6.7.3.2	Top organisational		1
Cybersecurity strategy	Section 6.7.3.3	Top organisational	Immaturity of cybersecurity roadmap / strategy	1
Policies, standards, and procedures	Section 6.7.3.4	Top Procedural		2
Compliance plan for legal and regulatory requirements	Section 6.7.3.5	Top Procedural		2
Cybersecurity structure with sufficient security resources for IIoT	Section 6.7.3.6	Top organisational	Inadequate staff supporting IIoT security	2
Vulnerability Management	Section 6.7.3.7	Top vulnerability	Old and new vulnerabilities	3

Control	Reference	Justification	Threat / Vulnerability / Risk	Phase
User and Device Access Management including Remote Access	Section 6.7.3.8	Top threat Top control	Unauthorised remote access, Insider and privilege misuse	3
Data encryption	Section 6.7.3.9	Top threat	Cyber espionage, Insider and privilege misuse	3
System Change Control	Section 6.7.3.10	Top threat	Insider and privilege misuse	3
Malware Protection	Section 6.7.3.11	Top threat	Malware (particular ransomware)	3
Segmentation (Firewall, standalone)	Section 6.7.3.12	Top threat Top control	Distributed Denial of Service (DDoS), Unauthorised remote access	3
Patch Management	Section 6.7.3.13	Top vulnerability Top control	No or delay in Patching/firmware updates	3
Systems hardening and Configuration Management	Section 6.7.3.14	Top vulnerability	Insecure Default Settings	3
Software Development	Section 6.7.3.15	Top vulnerability	Insecure mobile interface	3
Asset management	Section 6.7.3.16	Top vulnerability	legacy endpoints/devices	3
Secure communication	Section 6.7.3.17	Top Vulnerability Top control	Legacy communications / protocols	3
Redundancy/resilient infrastructure and	Section 6.7.3.18	Top risk Top threat	Unavailability of IIoT devices and / or networks Distributed Denial of Service (DDoS)	3
Backup and Recovery	Section 6.7.3.19	Top risk Top threat		3
Business Continuity and Disaster recovery plans	Section 6.7.3.20	Top risk Top threat		3
Physical Access control	Section 6.7.3.21	Top risk	Human safety, Safety regulations / considerations / consequences / implications.	3
Environmental Standards	Section 6.7.3.22	Top risk	Human safety, Safety regulations / considerations / consequences / implications.	3
Cybersecurity awareness program	Section 6.7.3.23	Top organisational	Immature security culture	3
Cybersecurity training program	Section 6.7.3.24	Top People		3
Monitoring (SIEM or Security Intelligence Centre and Audit logs)	Section 6.7.3.25	Top threat Top Risk Top Control	Cyber espionage, Unauthorised remote access, Insider and privilege misuse	4
Innovation Enablement Program	Section 6.7.3.26	Size & Structure	Lack of innovativeness culture	4
Incident Response Plan	Section 6.7.3.27	Top Procedural		4
Employee engagement program	Section 6.7.3.28	Top People		4
Employee satisfaction program	Section 6.7.3.29	Top People		4
Predictive Analytics and Board reporting	Section 6.7.3.30	To reach mature level		5
Continuous improvement and benchmarking	Section 6.7.3.31	To reach mature level		5

6.7.3.1 Risk Management

Perform an initial thorough assessment of the IIoT environment, including risk assessments and gap analyses. Evaluate current policies, controls, and procedures to identify areas requiring enhancement. Identify strengths, weaknesses, and potential risks to establish a foundation for improvement initiatives (Minett, 2022).

To enhance the maturity of risk management practices and establish a proactive approach to address the risks associated with IIoT technologies in the transport sector, the key phrases as discussed in Section 6.3.3 are used as guidance for the controls. The controls in relation to the factors are discussed below.

- **Technological** - Identify threats, risks and vulnerabilities that inform the risk posture of the organisation by conducting a thorough assessment of security risks associated with IIoT, considering data privacy, device vulnerabilities, network security, and operational risks. Develop a comprehensive threat model specific to the IIoT environment by identifying potential threats, their likelihood, impact, and potential attack vectors.
- **Organisational** – Develop a robust threat model specific to the IIoT environment to identify and analyse potential threats, and threat actors, understand their motivation, capabilities, likelihood, and impact, and map them to the organisation's risk appetite. Implement effective threat mitigation measures to align with the organisation's risk appetite. This includes implementing security controls, conducting regular vulnerability assessments and penetration testing, and leveraging threat intelligence to identify and mitigate emerging threats proactively. Ensure mitigation efforts are prioritised based on risk severity and aligned with the organisation's risk appetite. Regularly reassess the organisation's risk appetite considering new threats and adjust risk management strategies accordingly.
- **Procedural** – Develop a well-defined risk management strategy that encompasses the unique challenges and requirements of IIoT environments. This strategy should outline the organisation's methodology for managing risks, including:
    - risk appetite.
    - risk acceptance criteria.
    - outsourcing of risk.
    - risk avoidance.
    - risk transfer or mitigation and
    - risk tolerance levels specific to IIoT.
- **People** – Provide risk management training throughout the organisation. Foster a culture that encourages awareness and adherence to IIoT cybersecurity standards.

6.7.3.2 Executive Engagement Program

To establish a program for executive management to enhance the understanding and involvement of senior executives in IIoT security. Getting executive buy-in is critical to driving the implementation of cybersecurity controls. The tone at the top would ensure that security is incorporated into everything, such as strategic planning, budget, and resource allocation decisions (Uchendu et al., 2021). The key phrases discussed in Section 6.3 are used as guidance for the controls.

- **Technological** - Enable executives to make informed business decisions with the necessary information and insights. This includes involving senior executives in risk assessment (as discussed in Section 6.4), presenting the risks (discussed in Section 6.2.3), and discussing potential mitigation strategies.
- **Organisational** – As discussed in Section 6.3, the executive engagement programs would be informed by the organisation's size, structure, and executive management buy-in.
- **Procedural** – Develop a communication strategy to communicate the importance of IIoT security to senior executives. Clearly articulate the potential risks, business impacts, and strategic implications of inadequate security measures. Use concise and relevant language to convey the message and emphasise the role of senior executives in driving a strong security posture. Implement security metrics that provide insights into the effectiveness of IIoT security measures. Establish key performance indicators (KPIs) that align with business objectives and enable senior executives to assess the organisation's security posture. Regularly report these metrics to senior executives, highlighting areas of improvement, emerging threats, and the effectiveness of security initiatives.
- **People** – Foster an understanding of stakeholder expectations related to IIoT security among senior executives. Enable executives to make informed business decisions with the necessary information and insights. This includes involving senior executives in risk assessment, presenting risk scenarios, and discussing potential mitigation strategies. Encourage senior executives to prioritise IIoT security in decision-making processes. Promote a culture where security is seen as a critical enabler of business objectives and senior executives actively champion security initiatives. Identify and empower security evangelists among senior executives who can advocate for IIoT security within the organisation. These individuals can be role models, sharing their knowledge and experiences to inspire others to prioritise security. Encourage senior executives to actively participate in industry forums, conferences, and thought leadership events to stay updated on emerging security trends and technologies.

6.7.3.3 Develop a Comprehensive Cybersecurity Roadmap/Strategy

To ensure that the IIoT security and organisational strategies are aligned. The key phrases as discussed in Section 6.3.3 are used as guidance for the controls.

- **Technological -** Incorporate internal and external threats and risks (as discussed in Sections 6.2.1 & 6.2.3) into the cybersecurity roadmap/strategy, aligning it with the threat model developed under the procedural factors.
- **Organisational** – Define a clear and well-defined security model that outlines the organisation's approach to securing IIoT systems in the transport sector. Assess and improve the organisation's current security posture concerning IIoT. Clearly define the security objectives the organisation aims to achieve for its IIoT environment.
- **Procedural** – Develop a comprehensive threat model specific to the IIoT environment by identifying potential threats, their likelihood, impact, and potential attack vectors.
- **People** – Ensure the strategy include the number of resources required to execute it, e.g. size and structure of security staff (as discussed in Section 6.3.1)

6.7.3.4 Policies, Standards, and Procedures

To ensure adequate policies, standards and procedures are implemented and communicated to all relevant stakeholders to govern the IIoT environment. The key phrases as discussed in Section 6.4 are used as guidance for the controls.

- **Technological** – Ensure mechanisms, such as tools, are in place to monitor and report assurance activities to assess the effectiveness of governance processes for IIoT. This could include regular internal and external audits, compliance monitoring, vulnerability assessments, and penetration testing of IIoT systems.
- **Organisational** – Identify and understand the relevant regulatory and compliance requirements specific to IIoT in the transport sector and develop processes and controls to ensure compliance with these regulations and methods for monitoring and reporting compliance status.
- **Procedural** – Identify and understand the relevant regulatory and compliance requirements specific to IIoT in the transport sector and develop processes and controls to ensure compliance with these regulations and methods for monitoring and reporting compliance status. Implement robust configuration management standards for IIoT devices and systems and enforce secure configuration practices to minimise vulnerabilities and ensure consistency across IIoT deployments. Develop metrics and key performance indicators (KPIs) to measure the effectiveness of governance controls and continuously improve the security posture of IIoT.
- **People** – Define clear roles and responsibilities for IIoT governance and ensure alignment with overall organisational governance structures. Develop and communicate security policies covering all IIoT security and governance areas. Monitoring of KPIs to measure effectiveness of the controls.

6.7.3.5 Compliance Plan for Legal and Regulatory Requirements

Ensure a compliance plan is in place for legal and regulatory requirements.

- **Technological** – Ensure mechanisms, such as tools, are in place to monitor and report assurance activities to assess the effectiveness of governance processes for IIoT. This could include regular internal and external audits, compliance monitoring, vulnerability assessments, and penetration testing of IIoT systems.
- **Organisational** – Identify and understand the relevant regulatory and compliance requirements specific to IIoT in the transport sector and develop a compliance plan as discussed under procedural to ensure compliance with these regulations. Specific regulations might apply depending on the type of organisation, e.g. maritime transport might be subject to additional regulation compared to automotive. The type of devices would also influence the compliance plan, e.g. all mobile-enabled systems (GSM) must conform to the RICA Act (Government of Republic of South Africa, 2002b).
- **Procedural** – Ensure a compliance plan is in place for legal and regulatory requirements. Ensure that the IIoT environment adheres to relevant privacy regulations, such as the Protection of Personal Information Act (POPIA) (Government of Republic of South Africa, 2013), King IV (Institute of Directors in Southern Africa, 2009) and Electronic Communications and Transactions Act (ECTA) (Government of Republic of South Africa, 2002a), Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA) in South Africa (Government of Republic of South Africa, 2002b) and Cybercrimes Act (Government of Republic of South Africa, 2020). Ensure compliance with IT (Information Technology) and OT (Operational Technology) regulations that govern the use and integration of IIoT systems and adherence to Safety Regulations. Develop methods for monitoring and reporting compliance status.
- **People** – Define clear roles and responsibilities for the compliance plan as well as monitoring thereof. Training might be required for security staff dealing with regulations (refer to Section 6.7.3.24)

6.7.3.6 Cybersecurity Structure with Sufficient Security Resources for IIoT:

Ensure an adequate structure with skilled cybersecurity professionals to support IIoT. The key phrases as discussed in Section 6.3 are used as guidance for the controls.

- **Technological -** The security posture of the organisation influencing the size and composition of the IIoT security team are determined by the threats, vulnerabilities and risks discussed in Section 6.2. The required skills of the IIoT security team are determined by the types of tools and technology in the organisation.

- **Organisational** – When assessing the size and composition of the IIoT security team, take into account the following factors: number of IIoT devices deployed, industry type (e.g. the security needs of a transportation fleet management system may differ from those of a smart traffic management system), involvement of multiple organisations/divisions, and the security posture of the organisation.
- **Procedural** – Organisation's Human Resource (HR) procedures for recruitment needs to be followed.
- **People** – Ensure the structure contain skilled cybersecurity professionals to support IIoT.

6.7.3.7 Vulnerability Management

To ensure that vulnerabilities to IIoT systems are managed and minimised. The controls below are from the documents selected for analysed in Section 5.2.1, these include the Industrial Internet Consortium (2016).

- **Technological** – Vulnerability management tools are required for effective vulnerability management. Examples include commercial ICT vulnerability scanners such as Nessus and Qualys or more specialised IIoT scanners such as Microsoft Defender for IoT (Betts & Richards, 2023) and PIVoT Scan (Antrobus, Green, Frey, & Rashid, 2019).
- **Organisational** – Subscribe to external threat intelligence for early warnings of potential threats or newly discovered vulnerabilities. Apart from general security subscriptions, sector-specific subscriptions would depend on the type of organisation maritime transport would subscribe to, e.g., intelligence for shipping, and the automotive sector would subscribe to automotive intelligence.
- **Procedural** – Implement processes for continuous monitoring and remediation of new vulnerabilities in the IIoT landscape.
- **People** – Security staff would be required to perform vulnerability management using tools and would also need to be trained, as discussed in Section 6.7.3.24. Establish communication channels with vendors to receive timely notifications about security vulnerabilities. Continuously monitor and identify new vulnerabilities in the IIoT landscape. Stay updated on industry trends, vulnerabilities, and emerging attack techniques.

6.7.3.8 User and Device Access Management (including Remote Access)

This includes access to systems, devices, applications, databases, and equipment to ensure that new and terminated employees are managed in the IIoT environment. The controls below are from the documents selected for analysed in Section 5.2.1, these include the Industrial Internet Consortium (2016).

- **Technological** – Enable multi-factor authentication (MFA) (Vada, 2022) to access systems and devices. Use Virtual Private Networks (VPNs) or secure remote access gateways to establish secure connections (Pohl & Schotten, 2017).
- **Organisational** – Regularly perform and manage security reviews of all third parties with remote access to the IIoT. This consistent effort demonstrates the organisation's unwavering commitment to maintaining secure access controls, providing reassurance in the face of potential cyber threats.
- **Procedural** – Implement procedures for access to systems, devices, applications, databases, and equipment. Establishing procedures for enabling MFA and configuring encryption mechanisms for remote access ensures consistent security practices across the IIoT environment.
- **People** – Providing training and awareness programs on secure access management educates employees about the importance of following access control policies and procedures. Involving employees in security reviews of third-party access reinforces a culture of vigilance and shared responsibility for cybersecurity within the organisation. Ensure access is minimised to specific job functions.

6.7.3.9 Data Encryption

To ensure that critical and confidential data of the IIoT environment are protected via encryption.

- **Technological** - Encrypt sensitive data stored in a database, operating system, application, device, or mobile device and implement robust authentication mechanisms. Adopt encryption protocols for communication channels (wired or wireless) to safeguard critical and confidential data during transit and to mitigate the risk of interception by malicious actors. IIoT data can be encrypted using symmetric key encryption, such as AES (Qi, Lu, Wei, & Chen, 2020). Blockchain-enhanced security access control schemes can be considered where data are stored in IIoT cloud platforms (Yu, Tan, Aloqaily, Yang, & Jararweh, 2021).
- **Organisational** – The type of organisation and data confidentiality determines the control levels (McCallister, 2010). For example, data containing temperature readings is less critical than data containing instructions for moving transportation equipment.
- **Procedural** – One critical aspect is the implementation of procedures for regular monitoring and review of encrypted data. This ensures ongoing compliance with security standards and helps identify anomalies or potential security incidents. Additionally, establishing protocols for encrypting sensitive data on mobile devices and communication channels promotes consistency in security practices across the organisation.

- **People** – Providing training to security staff implementing encryption methods and awareness programs on the importance of data encryption to educate employees about their role in safeguarding critical and confidential information.

6.7.3.10 System Change Control

It is crucial to implement proper management of changes to IIoT systems and formal handling of data conversions by adhering to the Change and Release Management Procedure and System Development Lifecycle Methodology (Industrial Internet Consortium, 2016).

- **Technological** - Implement change control tools that automate the tracking and documentation of changes to IIoT systems. This will enhance efficiency and ensure that only authorised and tested changes are deployed to production environments. As discussed in Section 6.2.2, this will reduce the risk of introducing vulnerabilities.
- **Organisational** – Allocate resources, including personnel and budget, for change management activities to demonstrate the organisation's commitment to ensuring the reliability and security of IIoT systems.
- **Procedural** – Implement change and release management procedures and the System Development Lifecycle Methodology. Ensure that changes undergo thorough evaluation and approval before implementation, reducing the risk of unauthorised or untested changes.
- **People** – Providing training and education as part of user awareness (see Section 6.7.3.24) on the change and release management procedures.

6.7.3.11 Malware Protection

To ensure that the IIoT environment is protected against malware and external threats.

- **Technological** - Implement vendor-accredited and configured anti-malware software.
- **Organisational** – In cases where anti-malware software cannot be installed, alternative protective measures should be adopted, such as performing gateway anti-virus scanning or conducting manual checks on media (NIST, 2019).
- **Procedural** – Document and implement a process and standard for malware scanning, updating, and monitoring. Also, document a process where anti-malware software cannot be installed, and alternative protective measures should be adopted as mentioned above under organisational factors (NIST, 2019).
- **People** – Provide training to security staff to acquire the relevant skills for effective malware management (see Section 6.7.3.24). Educate the users as part of user awareness (see Section 6.7.3.23) about the dangers of malware and safe practices.

6.7.3.12 Segregation from other Networks and Firewalls in Place

To ensure that the IIoT environment is protected or segregated from other networks as per the top control mentioned in Section 6.7.2.1.

- **Technological -** Install, configure, and manage layer seven firewalls and Web application firewalls (WAF) to protect against DDoS attacks and other web application attacks.
- **Organisational** – Depending on the organisation's size, budget (e.g. where firewalls are costly), segmentation can be achieved via network subnets with unique security controls and protocols (Yatagha, Waedt, Schindler, & Kirdan, 2023).
- **Procedural** – Document and implement a process and firewalls standard, including rules, configuration, and monitoring. Also, document a process where firewalls cannot be installed, and the alternatives mentioned under organisational factors.
- **People** – Train security staff to acquire the relevant skills for effective firewall management and monitoring; refer to Section 6.7.3.24 for training.

6.7.3.13 Patch Management

Ensure a formal patch management process is in place to allow timely and regular updates for all IIoT devices and systems (Industrial Internet Consortium, 2016) and as per the top control mentioned in Section 6.7.2.1.

- **Technological** – a Patch management tool is recommended for effective patch management. Tools like SCCM, Solarwinds, and WSUS can be used depending on the underlying operating system. By utilising these tools, the patch management process can be streamlined to ensure the security of IIoT devices and systems.
- **Organisational** – Where it is not possible or practical to implement patches, alternative appropriate protection measures should be considered. As discussed in Section 6.3.3, the risk appetite would determine the prioritisation of patching efforts guided by regular vulnerability assessments.
- **Procedural** – Processes for patch management that include testing of all patches on a test environment before installing them on production systems. Where possible, automate patch management systems to streamline the process and reduce the risk of delays. Maintain an inventory of all devices and their firmware versions to track and schedule necessary updates. Regularly update and patch mobile applications to address any security vulnerabilities.
- **People** – IT or security staff would be required to perform patch management, depending on the roles & responsibilities. The staff would also need to be trained as discussed in Section 6.7.3.24. Establish communication channels with vendors to receive timely notifications about security patches and updates.

6.7.3.14 Systems Hardening and Configuration Management

Ensure that the IIoT devices and supporting infrastructure have been hardened (NIST, 2019).

- **Technological** – Change the default passwords and usernames on IIoT devices and systems to strong and unique credentials. Before deploying new IIoT systems, perform security assessments to identify and mitigate any insecure default settings.
- **Organisational** – As discussed in Section 6.3, the extent or robustness of configuration policies and procedures depends on the organisation's size, structure, and risk appetite.
- **Procedural** – Implement password policies, active security features, and disable unused services and ports in the operating systems and applications to prevent unauthorised use and reduce the attack surface (e.g. disable removable media such as USB drives where possible). Where removable media is necessary, procedures are in place to ensure these are checked for malware before use. Implement secure configuration practices, such as disabling unnecessary features or protocols. Review and update device configurations to ensure they align with security best practices. Ensure that the configuration of IIoT systems has been documented in a configuration management database (CMDB) and that no IIoT configuration changes are made without a corresponding CMDB update.
- **People** – Provide training to security staff to acquire the relevant skills for effective systems hardening and configuration management; refer to Section 6.7.3.24 on training.

6.7.3.15 Software Development

Ensure secure software development processes, such as DevSecOps, are implemented (Bahaa, Abdelaziz, Sayed, Elfangary, & Fahmy2021).

- **Technological -** DevSecOps encompasses tools and procedures (refer to procedural factor below) that promote cooperation among developers, security experts, and operations teams to develop effective and protected software. Implement digital signatures to verify the authenticity of application DLLs before they are executed, as well as code signing.
- **Organisational** – Depending on the organisation's size, structure, and risk appetite, as discussed in Section 6.3, this would shape the extent or robustness of configuration policies and procedures.
- **Procedural** – Implement a DevSecOps process that incorporates security testing throughout every phase of software development. Also, implement secure coding practices for applications (including mobile) interacting with IIoT devices.

- **People** – Provide training to security staff to conduct security testing and code reviews for IIoT applications (including mobile) to identify and fix vulnerabilities, refer to Section 6.7.3.24 on training.

6.7.3.16 Asset Management

Ensure a comprehensive asset register identifies all IIoT assets.

- **Technological** - Assess the risks associated with legacy endpoints/devices in the IIoT environment. Asset management tool would be recommended to assist with inventory management (Matsumoto et al., 2021).
- **Organisational** – As discussed in Section 6.3, the extent or robustness of asset management policies and procedures depends on the organisation's size, number of assets, and risk appetite.
- **Procedural** – Maintain a comprehensive asset register identifies all IIoT assets and their firmware versions to track and schedule necessary updates. Develop a plan to phase out or upgrade legacy devices to more secure and modern alternatives.
- **People** – Provide staff with training to maintain all IIoT assets applications (including mobile) and identify and fix vulnerabilities. Refer to Section 6.7.3.24 on training.

6.7.3.17 Secure Communication

Use secure communication protocols for data transmission to and from IIoT devices as per the top control mentioned in Section 6.7.2.1.

- **Technological** - Use secure communication protocols (e.g., HTTPS) for data transmission to and from IIoT devices. Identify and assess the risks associated with legacy communications and protocols used in the IIoT environment. Where feasible, transition to more secure communication protocols, such as TLS or secure VPNs. Disable or restrict the use of insecure protocols or implement additional security measures (e.g., encryption, authentication) for legacy protocols. Implement network monitoring and intrusion detection systems to detect and block malicious activities targeting legacy communications (Baruah & Dhal, 2020).
- **Organisational** – Depending on the organisation's size, number of assets, type of devices and risk appetite as discussed in Section 6.3, this would shape the extent or robustness of communication protocols.
- **Procedural** – Regularly review and update protocols to ensure security standards and best practices compliance. It is crucial to minimise the usage of wireless networks and maintain regular monitoring and review of wireless connections.
- **People** – Provide training to staff to manage, implement and monitor secure communication methods to and from all IIoT devices, refer to Section 6.7.3.24 on training.

6.7.3.18 Redundancy and Resilient Infrastructure

Redundancy and resilient infrastructure (H. Wu, Miao, Zhang, Tian, & Tian, 2022) exists for critical IIoT environments, systems, equipment, and components. These include redundant networks, switches, servers, workstations, and devices. Implement redundancy and failover mechanisms to maintain service availability during example, a DDoS attack (Laszka, Abbas, Vorobeychik, & Koutsoukos, 2020).

- **Technological** - Implement redundancy and failover mechanisms to maintain service availability during for example, a DDoS attack.
- **Organisational** – As discussed in Section 6.3, the extent or robustness of the redundancy standard depends on the organisation's size, number of assets, type of devices, and risk appetite.
- **Procedural** – Implement standards for redundancy of critical IIoT environments, systems, equipment, and components. These include redundant networks, switches, servers, workstations, and devices.
- **People** – Provide training to staff to manage, implement and monitor redundancy and failover mechanisms for IIoT devices; refer to Section 6.7.3.24 on training.

6.7.3.19 Backup and Recovery

Ensure that adequate backups and recovery procedures are in place (H. Wu et el., 2022).

- **Technological** - Implement tools to perform backups.
- **Organisational** – The size, number of assets, type of devices, and risk appetite of the organisation, as discussed in Section 6.3, are key factors that shape the scope of the backup and recovery plan. This ensures the plan is tailored to the organisation's specific needs and circumstances, ranging from local backups on disk or tape to backups in the cloud (H. Wu et el., 2022).
- **Procedural** – Ensure that adequate backups and recovery procedures are in place to safeguard critical data and that the integrity of backups is regularly tested.
- **People** – Provide staff with training to manage and monitor backup and recovery for IIoT devices; refer to Section 6.7.3.24 on training.

6.7.3.20 Business Continuity and Disaster Recovery Plans

To ensure recovery of IIoT systems to minimise business impact in the event of a significant disruption (Industrial Internet Consortium, 2016).

- **Technological** – A risk-based approach would inform the Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

- **Organisational** – The scope of the DRP and BCP would depend on the organisation's size, number of assets, type of devices, and risk appetite, as discussed in Section 6.3.
- **Procedural** – A DRP and BCP are developed in cooperation with business process owners and based on a risk-based approach and should clearly define the roles and responsibilities of the recovery team members. The DRP and BCP should be tested and updated to ensure the recovery of IIoT systems to minimise business impact in the event of a significant disruption.
- **People** – Engage with business process owners to develop the DRP and BCP. Train staff to manage and monitor backup and recovery for IIoT devices; refer to Section 6.7.3.24 for training.

6.7.3.21 Physical Access

To guarantee sufficient physical security, it is vital to implement appropriate measures that limit access to areas containing IIoT equipment and devices, as guided by the Industrial Internet Consortium (2016).

- **Technological** – Improve physical security by implementing access control systems, surveillance cameras, and security guards at critical locations. Implement tamper-evident seals or locks to identify and deter physical tampering attempts.
- **Organisational** – As discussed in Section 6.3, the organisation's size, structure, number of locations, and risk appetite would inform the physical access control policies and procedures. For example, sites containing critical equipment or data might require security guards, whereas less critical sites might only require access controls.
- **Procedural** – Establish strict access control policies and procedures to restrict physical access to IIoT devices and infrastructure.
- **People** – Conduct regular inspections and maintenance of physical security measures to ensure it remains secure. Provide training to staff to manage and monitor physical security access controls for IIoT devices, refer to Section 6.7.3.24 on training. Educate the users as part of user awareness (see Section 6.7.3.23) around the dangers of physical access controls and what safe practices to follow.

6.7.3.22 Environmental Standards

Ensure a resilient infrastructure with necessary facilities is installed to protect the IIoT systems (Industrial Internet Consortium, 2016).

- **Technological** – Implement environmental controls such as UPS/generators, fire suppression equipment, and air conditioners to ensure equipment resides in environmentally controlled areas at appropriate ambient conditions to ensure proper and sustainable operation.

- **Organisational** – As discussed in Section 6.3, the organisation's size, structure, number of locations, and risk appetite would inform its environmental policies and procedures. For example, sites containing critical equipment or data might require generators, whereas less critical sites might only require a UPS.
- **Procedural** – Establish environmental policies and procedures to ensure IIoT equipment resides in environmentally controlled areas.
- **People** – Conduct regular inspections and maintenance of facilities hosting IIoT devices to ensure they remain in appropriate ambient conditions. Train staff to manage and monitor facilities hosting IIoT devices; refer to Section 6.7.3.24 for training.

6.7.3.23 Security Awareness Program

To enhance awareness and skills, it is crucial to conduct continuous and comprehensive awareness programs for all employees. The key phrases discussed in Section 6.5 are used as guidance for the controls.

- **Technological** – Awareness training can be conducted through newsletters, internal bulletins, or online platforms. Implement tools to conduct regular phishing simulations.
- **Organisational** – The cybersecurity awareness programs would be informed by the organisation's size, structure, risk appetite, and security culture, as discussed in Section 6.3. For example, organisations lacking a mature security culture would require a more intense cyber awareness program.
- **Procedural** – Establish cybersecurity awareness programs. These programs should emphasise the significance of security awareness, specifically for IIoT environments. This includes raising awareness about potential threats, best practices for securing IIoT devices, the impact of individual actions on overall security and conducting situational awareness programs to educate employees on recognising and responding to security incidents or reporting suspicious activities related to IIoT.
- **People** – Conduct continuous and comprehensive security awareness training and educational programs for all employees. Promote a culture of accountability and responsibility by clearly defining roles and responsibilities related to IIoT security. Establish regular communication channels to disseminate security-related information, updates, and best practices to all stakeholders. Encourage employees to actively engage in security discussions and provide feedback or suggestions to improve IIoT security practices. Regularly assess the effectiveness of the security awareness program and seek feedback from employees. Use this feedback to improve the program and address any gaps identified. Regular phishing simulations should be conducted to identify users who fell victim to these and provide additional training.

6.7.3.24 Cybersecurity Training Program

Ensure there are cybersecurity training programs that covering all relevant employees. The key phrases as discussed in Section 6.5 are used as guidance for the controls.

- **Technological** –Training can be done in person, online or through platforms.
- **Organisational** – As discussed in Section 6.3, the cyber training programs would be guided by the organisation's size and structure.
- **Procedural** – Establish cybersecurity training programs that range from general employees interacting with IIoT to security professionals dealing with IIoT. This will minimise human error and increase investment in expertise. The training programs for employees should focus on general security skills highlighting the importance of security, risk management, and incident response. Develop specialised training programs that focus specifically on IIoT security. Continuously evaluate the effectiveness of the training programs and make necessary improvements.
- **People** – Establish a culture of continuous learning and professional development by encouraging employees to pursue certifications, attend industry conferences, and participate in workshops and webinars related to general security and IIoT security.

6.7.3.25 Monitoring (SIEM or Security Intelligence Centre and Audit logs)

Ensure that regular system monitoring of the IIoT environment is performed as discussed in Section 2.2.3.1.

- **Technological -** At a minimum, audit logs should be enabled and reviewed to monitor access and remote access activities for suspicious behaviour or unauthorised access. A more mature control is to have a SIEM or Security Intelligence Centre (SIC). An application to run the SIEM would be required, and the size would depend on the organisational factors.
- **Organisational** – The size and structure of the organisation, i.e. number of devices, security posture, as discussed in Section 6.3, would determine the extent of the control implementation. Monitoring audit logs for multiple devices and geographically dispersed systems would be difficult compared to an SIEM solution.
- **Procedural** – Implement a process for event monitoring, detection, and remediation. This includes network traffic and user access (including remote access) to detect suspicious behaviour, indicators of compromise, and anomalies to detect and block sophisticated attacks.
- **People** – Security staff would be required to review the audit logs or monitor the SIEM / SIC. The number of staff is dependent on organisational factors. For example, an organisation running 24/7 would need multiple shifts compared to an organisation running 9 am to 5pm, which would require one shift. The staff would also need to be trained, as discussed in Section 6.7.3.24.

6.7.3.26 Innovation Enablement Program

It is crucial to establish an innovation enablement program. The key phrases, as discussed in Section 6.3, serve as essential guidance for the controls.

- **Technological** – Online platforms to encourage innovation and tools to capture innovative ideas can be deployed.
- **Organisational** – As discussed in Section 6.3, the innovation enablement programs would be informed by the organisation's size, structure, and innovativeness culture. For example, organisations lacking a mature innovative culture would require a more intense innovation enablement program.
- **Procedural** – Establish an innovation enablement program that fosters an innovative culture within the organisation and promotes the adoption of innovative practices specific to IIoT security.
- **People** – Establish a culture of innovation by creating platforms and channels that facilitate employee collaboration and sharing expertise and experiences regarding IIoT. This can include forums, workshops, or innovation hubs where employees can brainstorm ideas, exchange knowledge, and work together to find innovative solutions for securing IIoT systems.

6.7.3.27 Incident Response Plan

Ensure that response capabilities to IIoT system incidents are understood and managed. The key phrases discussed in Section 6.4 guide the controls.

- **Technological** – Implement a helpdesk system to prioritise and track incidents and escalation of long outstanding incidents. Monitor emerging IIoT threats and adapt the incident response procedures to address new risks and vulnerabilities as they arise.
- **Organisational** – The size and structure of the organisation, i.e. the number of devices and security posture, as discussed in Section 6.3, would determine the extent of the control implementation. For multiple devices and geographically dispersed systems, multiple teams would be required.
- **Procedural** – Implement procedures to escalate an incident to a disaster and invoke BCP or DRP where required. This will improve the maturity of the organisational incident response plan and ensure it adequately addresses the risks associated with IIoT. Consider the following factors when enhancing the incident response plan. Implement comprehensive monitoring and analysis techniques specific to IIoT environments. This includes rule-based analysis, forensic analysis, root cause analysis, behavioural analysis, and monitoring of encrypted channels. Incorporate these techniques into the incident response plan to enable effective detection, analysis, and response to security incidents involving IIoT systems.

- **People** – Conduct periodic testing and evaluation of the incident response plan's effectiveness using tabletop exercises, simulations, and drills to ensure readiness in responding to incidents. Identify gaps and areas of improvement and update the plan. The staff involved with incident management would also need to be trained, as discussed in Section 6.7.3.24

6.7.3.28 Employee Engagement

Ensure an employee engagement program is in place. The key phrases, as discussed in Section 6.5, are used as guidance for the controls.

- **Technological** – Online platforms such as MS Team or Zoom can be used for engagement.
- **Organisational** – The employee engagement programs would be informed by the organisation's size and structure and whether employees are engaged, as discussed in Section 6.3.
- **Procedural** – Develop an employee engagement program to establish communication channels and build relationships between engineering/OT and security staff, IT and security staff, management and security staff and executive engagement with security staff. The program should additionally deliver training and promote awareness, integrating security considerations into workflows and decision-making processes. Include security metrics and reporting mechanisms in management KPIs to provide security posture and progress visibility.
- **People** – The employee engagement program should cultivate a culture that prioritises security awareness and fosters a sense of accountability. Encourage regular meetings and discussions between management and security staff to review security strategies, initiatives, and risk mitigation plans. Arrange periodic executive briefings and presentations by security staff to provide insights into emerging security threats, industry trends, and the organisation's security posture. Provide executive management with regular reports on the effectiveness of security controls and risk management efforts.

6.7.3.29 Employee Satisfaction Program

Ensure employee recognition and reward programs are in place. The key phrases, discussed in Section 6.5, guide the controls.

- **Technological** – Invest in robust, user-friendly tools and technologies that effectively enable employees to manage IIoT security.
- **Organisational** – Depending on the organisation's size, structure, and whether employees are satisfied as discussed in Section 6.3, this would inform the employee satisfaction programs.
- **Procedural** – Develop and implement employee recognition and reward programs to acknowledge and incentivise exceptional performance, fostering a positive work environment and job satisfaction. This should also include an effective communication strategy to address

employee concerns and provide regular updates on organisational goals, strategies, and progress. Establish channels for employees to provide feedback and suggestions and express concerns about their work environment, job satisfaction, and IIoT security. Conduct employee satisfaction surveys periodically to gather insights and identify areas for improvement. Implement employee recognition programs to acknowledge and reward exceptional performance, fostering a positive work environment and job satisfaction. Implement policies and practices that promote work-life balance and employee well-being. Offer avenues for professional development and advancement to boost employee motivation and engagement.

- **People** – Provide comprehensive training and support to employees on adequately using these tools and technologies. Regularly assess the effectiveness and usability of the tools and make necessary improvements based on employee feedback. Foster a positive work environment encouraging collaboration, open communication, and teamwork. Ensure that employees have the necessary resources, training, and support to perform their roles effectively in the IIoT environment. Regularly assess employee workload and adjust to prevent burnout and optimise productivity.

6.7.3.30 Predictive Analytics and Board reporting

- **Technological** – Utilise advanced anomaly detection systems to identify suspicious patterns or unauthorised access attempts within IIoT infrastructure. Use tools such as MS Power BI for board reporting.
- **Organisational** – Develop a robust model specific to the IIoT environment to identify security-related data that could be used for predictive analytics to be able to ward off a potential attack at an early stage as well as reporting (Empl & Pernul, 2021). These include KPIs, threats, incidents, vulnerabilities, and risks.
- **Procedural** – Develop a process for action and follow up on the predictive analytics results. Also, security KPIs should be developed to provide the board with visibility into its security posture and progress.
- **People** – Provide security staff with training on predictive analytics and reporting to acquire the relevant skills for effective incident management (see Section 6.7.3.24).

6.7.3.31 Continuous improvement and benchmarking

- **Technological** – Perform regular assessments such as CMM (discussed in Section 2.2.3.2) to improve the IIoT control and risk environment. This includes identifying threats, risks, and vulnerabilities through an assessment that would inform the risk profile and maturity. Use these to benchmark against other organisations.

  Organisational – Establish a formal continuous monitoring program that defines key performance indicators (KPIs), metrics, and thresholds for assessing the organisation's

security posture on an ongoing basis (Adaros Boye et al., 2018). Ensure security policies and procedures are updated regularly based on continuous monitoring and compliance requirements.

- **Procedural** – Implement regular security assessments and penetration testing exercises (as mentioned under technological) to evaluate security controls' effectiveness and identify improvement areas in the continuous monitoring and benchmarking processes.
- **People** – Provide training to the security staff involved with continuous improvement and benchmarking.

6.7.4 Validate and Review Cybersecurity Framework

The MITRE ATT&CK framework, as discussed in Section 2.4.7.1, is a comprehensive and globally recognised knowledge base that provides insights into the tactics, techniques, and procedures (TTPs) used by cyber adversaries during various stages of an attack (The MITRE Corporation, 2023c).

It is essential to understand the tactics and techniques used by adversaries targeting IoT devices and systems. By leveraging the MITRE ATT&CK framework for ICS, organisations can adapt and extend its principles to address the unique challenges IoT environments pose. This framework enables IoT stakeholders to enhance their security posture, detect and respond to IoT-related threats, and mitigate the risks associated with cyberattacks on IoT infrastructure (Malware News, 2020). Microsoft also used the MITRE ATT&CK for ICS to validate the Azure Defender for IoT (Abdelaal, 2021). The ATT&CK framework for ICS is used to create an IIoT system attack tree and understand the cyber risk's impact on IIoT (Chapman, 2022).

6.7.4.1 Gap Analysis

The MITRE ATT&CK for ICS is used to validate the cybersecurity framework developed in 6.7.6 to determine if the techniques used by attackers are mitigated. The coding is as follows: red if the techniques used by attackers are not mitigated by control/s in the cybersecurity framework (this means that the risk are not addressed at all), orange if control/s in the cybersecurity framework partially mitigate the techniques used by attackers (this means that the risk are not addressed fully and there are residual risk that needs to be addressed), and green if control/s in the cybersecurity framework mitigated the techniques used by attackers (this means that the risk are fully addressed). The results are displayed in Figure 6.18 and Table 6.10.

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Figure 6-18: Gap analysis of Cybersecurity framework compared to MITRE ATT&CK framework

Source: Author compiled, Adapted from MITRE ATT&CK (The MITRE Corporation, 2023c)

Table 6-10: MITRE ATT&CK vs Cybersecurity framework

MITRE ATT&CK Tactic	Technique	Mitigated	Control from framework
Initial Access	Drive-by Compromise	Yes	Segmentation (Firewall, standalone) Malware Protection Patch Management
	Exploit Public-Facing Application	Yes	Segmentation (Firewall, standalone) User and Device Access Management including Remote Access Patch Management Vulnerability Management
	Exploitation of Remote Services	Yes	Segmentation (Firewall, standalone) User and Device Access Management including Remote Access Patch Management Vulnerability Management
	External Remote Services	Yes	Segmentation (Firewall, standalone) User and Device Access Management including Remote Access Vulnerability Management
	Internet Accessible Device	Yes	User and Device Access Management including Remote Access Segmentation (Firewall, standalone) Systems hardening and Configuration Management
	Remote Services	Yes	User and Device Access Management including Remote Access Segmentation (Firewall, standalone) Systems hardening and Configuration Management
	Replication Through Removable Media	Yes	Systems hardening and Configuration Management Malware Protection
	Rogue Master	Yes	User and Device Access Management including Remote Access Segmentation (Firewall, standalone)
	Spear phishing Attachment	Yes	Malware Protection Cybersecurity awareness program
	Supply Chain Compromise	Partially	Policies, standards, and procedures Plan for legal and regulatory requirements Software Development Patch Management Vulnerability Management
	Transient Cyber Asset	Yes	Malware Protection Policies, standards, and procedures Data encryption Segmentation (Firewall, standalone) Patch Management Secure communication
	Wireless Compromise	Yes	Data encryption Secure communication
Execution	Change Operating Mode	Yes	System Change Control User and Device Access Management including Remote Access Secure communication Segmentation (Firewall, standalone)
	Command-Line Interface	Yes	Systems hardening and Configuration Management

MITRE ATT&CK Tactic	Technique	Mitigated	Control from framework
			Malware Protection
	Execution through API	Yes	User and Device Access Management including Remote Access
	Graphical User Interface	Yes	User and Device Access Management including Remote Access Monitoring (SIEM or Security Intelligence Centre and Audit logs)
	Hooking	Yes	Policies, standards, and procedures Software Development
	Modify Controller Tasking	Yes	Policies, standards, and procedures Software Development
	Native API	Yes	Malware protection Secure communication
	Scripting	Yes	Malware protection
	User Execution	Yes	Malware protection Software Development Monitoring (SIEM or Security Intelligence Centre and Audit logs) Segmentation (Firewall, standalone) Cybersecurity awareness program
Persistence	Hardcoded Credentials	Yes	User and Device Access Management including Remote Access Systems hardening and Configuration Management
	Modify Program	Yes	User and Device Access Management including Remote Access Policies, standards, and procedures Software Development
	Module Firmware	Yes	Policies, standards, and procedures Software Development Secure communication Data encryption Segmentation (Firewall, standalone)
	Project File Infection	Yes	Policies, standards, and procedures Software Development Data encryption User and Device Access Management including Remote Access
	System Firmware	Yes	User and Device Access Management including Remote Access Policies, standards, and procedures Software Development Secure Communication Data encryption Segmentation (Firewall, standalone) Patch Management
	Valid Accounts	Yes	User and Device Access Management including Remote Access Monitoring (SIEM or Security Intelligence Centre and Audit logs) Policies, standards, and procedures Software Development
Privilege Escalation	Exploitation for Privilege Escalation	Yes	Vulnerability management Risk Management Malware Protection Patch Management
	Hooking	Yes	Policies, standards, and procedures

MITRE ATT&CK Tactic	Technique	Mitigated	Control from framework
			Software Development
Evasion	Change Operating Mode	Yes	System Change Control User and Device Access Management including Remote Access Secure communication Segmentation (Firewall, standalone)
	Exploitation for Evasion	Yes	Vulnerability management Risk Management Malware Protection Patch Management
	Indicator Removal on Host	Yes	User and Device Access Management including Remote Access
	Masquerading	Yes	Malware Protection User and Device Access Management including Remote Access Software Development
	Rootkit	Yes	Policies, standards, and procedures Software Development
	Spoof Reporting Message	Yes	Secure communication Segmentation (Firewall, standalone) User and Device Access Management including Remote Access
Discovery	Network Connection Enumeration	Yes	Segmentation (Firewall, standalone) Monitoring (SIEM or Security Intelligence Centre and Audit logs)
	Network Sniffing	Yes	Secure communication Segmentation (Firewall, standalone) User and Device Access Management including Remote Access Monitoring (SIEM or Security Intelligence Centre and Audit logs)
	Remote System Discovery	Yes	Segmentation (Firewall, standalone) User and Device Access Management including Remote Access
	Remote System Information Discovery	Yes	Segmentation (Firewall, standalone) User and Device Access Management including Remote Access
	Wireless Sniffing	Yes	Data encryption Secure communication
Lateral Movement	Default Credentials	Yes	User and Device Access Management including Remote Access Systems hardening and configuration management
	Exploitation of Remote Services	Yes	Segmentation (Firewall, standalone) User and Device Access Management including Remote Access Patch Management Vulnerability Management
	Hardcoded Credentials	Yes	User and Device Access Management including Remote Access Systems hardening and configuration management
	Lateral Tool Transfer	Yes	Monitoring (SIEM or Security Intelligence Centre and Audit logs) Segmentation (Firewall, standalone)

MITRE ATT&CK Tactic	Technique	Mitigated	Control from framework
	Program Download	Yes	User and Device Access Management including Remote Access Policies, standards, and procedures Software Development Secure Communication Segmentation (Firewall, standalone) Systems hardening and configuration management
	Remote Services	Yes	User and Device Access Management including Remote Access Segmentation (Firewall, standalone) Systems hardening and Configuration Management
	Valid Accounts	Yes	User and Device Access Management including Remote Access Monitoring (SIEM or Security Intelligence Centre and Audit logs) Policies, standards, and procedures Software Development
Collection	Adversary-in-the-Middle	Yes	Policies, standards, and procedures Secure communication User and Device Access Management including Remote Access Segmentation (Firewall, standalone)
	Automated Collection	Yes	Segmentation (Firewall, standalone)
	Data from Information Repositories	Yes	Policies, standards, and procedures Data encryption Monitoring (SIEM or Security Intelligence Centre and Audit logs) User and Device Access Management including Remote Access Cybersecurity awareness program
	Data from Local System	Partially	Data encryption Monitoring (SIEM or Security Intelligence Centre and Audit logs) User and Device Access Management including Remote Access Cybersecurity awareness program
	Detect Operating Mode	Yes	User and Device Access Management including Remote Access Secure communication Segmentation (Firewall, standalone)
	I/O Image	Partially	User and Device Access Management including Remote Access Physical Access control Secure communication
	Monitor Process State	No	None
	Point & Tag Identification	Yes	User and Device Access Management including Remote Access Secure communication Segmentation (Firewall, standalone)
	Program Upload	Yes	User and Device Access Management including Remote Access Secure communication Segmentation (Firewall, standalone)
	Screen Capture	Partially	User and Device Access Management including Remote Access

MITRE ATT&CK Tactic	Technique	Mitigated	Control from framework
			Monitoring (SIEM or Security Intelligence Centre and Audit logs) Systems hardening and configuration management
	Wireless Sniffing	Yes	Data encryption Secure communication
Command and Control	Commonly Used Port	Yes	Systems hardening and configuration management Segmentation (Firewall, standalone)
	Connection Proxy	Yes	Secure communication Segmentation (Firewall, standalone)
	Standard Application Layer Protocol	Yes	Secure communication Segmentation (Firewall, standalone)
Inhibit Response Function	Activate Firmware Update Mode	Yes	User and Device Access Management including Remote Access Secure communication Segmentation (Firewall, standalone)
	Alarm Suppression	Yes	Segmentation (Firewall, standalone)
	Block Command Message	Yes	Segmentation (Firewall, standalone)
	Block Reporting Message	Yes	Secure communication Segmentation (Firewall, standalone)
	Block Serial COM	Yes	Secure communication Segmentation (Firewall, standalone)
	Change Credential	Yes	Backup and Recovery Business Continuity and Disaster recovery plans Systems hardening and Configuration Management
	Data Destruction	Yes	Backup and Recovery User and Device Access Management including Remote Access
	Denial of Service	Yes	Segmentation (Firewall, standalone)
	Device Restart/Shutdown	Yes	User and Device Access Management including Remote Access Systems hardening and Configuration Management Secure communication Segmentation (Firewall, standalone)
	Manipulate I/O Image	Partially	Secure communication User and Device Access Management including Remote Access Physical Access control
	Modify Alarm Settings	Yes	User and Device Access Management including Remote Access Segmentation (Firewall, standalone)
	Rootkit	Yes	Policies, standards, and procedures Software Development
	Service Stop	Yes	User and Device Access Management including Remote Access Segmentation (Firewall, standalone)
	System Firmware	Yes	User and Device Access Management including Remote Access Policies, standards, and procedures Software Development Secure Communication Data encryption

MITRE ATT&CK Tactic	Technique	Mitigated	Control from framework
			Segmentation (Firewall, standalone) Patch Management
Impair Process Control	Brute Force I/O	Yes	User and Device Access Management including Remote Access Segmentation (Firewall, standalone)
	Modify Parameter	Yes	Policies, standards, and procedures Software Development User and Device Access Management including Remote Access System Change Control
	Module Firmware	Yes	Policies, standards, and procedures Software Development Secure communication Data encryption Segmentation (Firewall, standalone)
	Spoof Reporting Message	Yes	Secure communication Segmentation (Firewall, standalone) User and Device Access Management including Remote Access
	Unauthorised Command Message	Yes	Secure communication Segmentation (Firewall, standalone) User and Device Access Management including Remote Access Software Development
Impact	Damage to Property	Yes	Physical Access control Environmental Standards Segmentation (Firewall, standalone)
	Denial of Control	Yes	Backup and Recovery Business Continuity and Disaster recovery plans
	Denial of View	Yes	Backup and Recovery Business Continuity and Disaster recovery plans
	Loss of Availability	Yes	Backup and Recovery Business Continuity and Disaster recovery plans
	Loss of Control	Yes	Backup and Recovery Business Continuity and Disaster recovery plans
	Loss of Productivity and Revenue	Yes	Backup and Recovery Business Continuity and Disaster recovery plans
	Loss of Protection	Yes	Physical Access control Environmental Standards Backup and Recovery Business Continuity and Disaster recovery plans
	Loss of Safety	Yes	Physical Access control Environmental Standards
	Loss of View	Yes	Physical Access control Environmental Standards
	Manipulation of Control	Yes	Secure communication Backup and Recovery Business Continuity and Disaster recovery plans
	Manipulation of View	Yes	Secure communication

MITRE ATT&CK Tactic	Technique	Mitigated	Control from framework
			Backup and Recovery Business Continuity and Disaster recovery plans
	Theft of Operational Information	Yes	Data encryption User and Device Access Management including Remote Access Monitoring (SIEM or Security Intelligence Centre and Audit logs)

Legend

Colour	Explanation
Green	Control/s in the cybersecurity framework mitigated the techniques used by attackers.
Orange	Control/s in the cybersecurity framework partially mitigate the techniques used by attackers.
Red	The techniques used by attackers are not mitigated by control/s in the cybersecurity framework.

6.7.4.2 Addressing the Gaps

The gaps identified when validating the cybersecurity framework for IIoT to the MITRE ATT&CK tactics are displayed in Table 6.11.

Table 6-11: MITRE ATT&CK vs Cybersecurity framework gaps

MITRE ATT&CK Tactic	Technique	Gap	Corrective or additional control
Initial Access	Supply chain compromise	Partially mitigated. Missing supply chain management.	Supply chain management, see Section 6.7.4.2.1
Collection	Data from Local System	Partially mitigated. Missing Data Loss Prevention (DLP)	Data Loss Prevention, see Section 6.7.4.2.2
	I/O Image	Partially mitigated. As per MITRE ATT&CK (The MITRE Corporation, 2020a): "this technique may not be effectively mitigated against, consider controls for assets and processes that lead to the use of this technique."	Controls for assets and processes that lead to the use of this technique is listed, namely: Secure communication (see Section 6.7.3.17), User and Device Access Management including Remote Access (see Section 6.7.3.8), and Physical Access control (see Section 6.7.3.21). No further controls are required.
	Monitor Process State	As per MITRE ATT&CK (The MITRE Corporation, 2020b): "this type of attack technique cannot be easily mitigated with preventive controls since it is based on	No further controls are required.

MITRE ATT&CK Tactic	Technique	Gap	Corrective or additional control
		the abuse of system features."	
	Screen Capture	Partially mitigated. As per MITRE ATT&CK (The MITRE Corporation, 2020c): "Preventing screen capture on a device may require disabling various system calls supported by the operating systems (e.g., Microsoft WindowsGraphicsCaputer APIs), however, these may be needed for other critical applications."	Controls for disabling various system calls is listed, namely: User and Device Access Management including Remote Access (see Section 6.7.3.8), Monitoring (SIEM or Security Intelligence Centre and Audit logs) (see Section 6.7.3.25), Systems hardening and configuration management (see Section 6.7.3.14). No further controls are required.
Inhibit Response Function	Manipulate I/O Image	Partially mitigated. As per MITRE ATT&CK (The MITRE Corporation, 2020d): "this technique may not be effectively mitigated against, consider controls for assets and processes that lead to the use of this technique."	Controls for assets and processes that lead to the use of this technique is listed, i.e. Secure communication (see Section 6.7.3.17), User and Device Access Management including Remote Access (see Section 6.7.3.8), and Physical Access control (see Section 6.7.3.21). No further controls are required.
Impact	Theft of Operational information	Partially mitigated. Missing DLP	Data Loss Prevention, see Section 6.7.4.2.2

Stemming from the gap analysis, the following controls are added to the cybersecurity framework developed in 6.7.6:

6.7.4.2.1 Supply Chain Management:

The controls listed under supply chain management as part of the Mitre framework (The MITRE Corporation, 2023a) mitigations are partially covered as per Table 6.12 below.

Table 6-12: Supply chain management mitigations

MITRE ID	MITRE Mitigation	Cybersecurity framework reference where covered
M0947	Audit	Policies, standards, and procedures (Section 6.7.3.4) compliance plan for legal and regulatory requirements Section 6.7.3.5)
M0945	Code Signing	Software Development (Section 6.7.3.15)
M0817	Supply Chain Management	None
M0951	Update Software	Patch Management (Section 6.7.3.13)
M0916	Vulnerability Scanning	Vulnerability Management (Section 6.7.3.7)

The supply chain management are not covered by the cybersecurity framework in Section 6.7.3. This control would need to be implemented as there is a risk around third-party vendors or suppliers. From the Target incident discussed in Section 2.4.6, a vendors or third-party services were compromised to gain access to the organisation. The following control needs to be implemented to fully address the risk:

Ensure effective supply chain management programs are in place which incorporate approaches to evaluate the reliability and technological advancement of a supplier (The MITRE Corporation, 2023a).

- **Technological -** Incorporate supply chain management risks (NIST, 2019) into the supply chain management program developed under the procedural factors.
- **Organisational** – Depending on the organisation's size, number of assets, number of vendors and risk appetite as discussed in Section 6.3, this would shape the scope of the supply chain management programs.
- **Procedural** – Develop effective supply chain management programs which incorporate approaches to evaluate the reliability and technological advancement of a supplier. It should also encompass technical measures like code-signing (as discussed in Section 6.7.3.15) and bill of materials to ensure the integrity of newly acquired devices and components. It is essential to develop procurement language that highlights the anticipated requirements from suppliers concerning artefacts, audit records, and technical capabilities necessary to validate the integrity of the device supply chain (The MITRE Corporation, 2023a).
- **People** – Provide training to staff dealing with the supply chain ensuring they are aware of the risks and requirements from the supply chain management program.

6.7.4.2.2 Data Loss Prevention

The controls listed under Data Loss Prevention as part of the Mitre framework (The MITRE Corporation, 2023b) mitigations are partially covered as per Table 6.13 below.

Table 6-13: Data loss prevention mitigations

MITRE ID	MITRE Mitigation	Cybersecurity framework reference where covered
T0893	Data from Local System	Partially covered under Data Encryption (see Section 6.7.3.9). Although data encryption can protect the data, it does not contain methods to detect critical data that is not encrypted, whereas DLP can (The MITRE Corporation, 2023b).
T0882	Theft of Operational Information	Partially covered under User and Device Access Management including Remote Access (see Section 6.7.3.8). Access control focuses on controlling access to data or information (Microsoft, n.d.), whereas DLP is concerned with preventing

MITRE ID	MITRE Mitigation	Cybersecurity framework reference where covered
		unauthorised disclosure or leakage of sensitive data (Immuta, n.d.).

The DLP risks are fully covered by the cybersecurity framework in Section 6.7.3. This control would need to be implemented as there is a risk around cyber espionage compromising trade secrets and sensitive information (as discussed in Section 6.2.3). The following control needs to be implemented to fully address the risk:

Implement a DLP system to detect malicious attempts to exfiltrate organisational data.

- **Technological** - Implement a DLP system to detect malicious attempts to exfiltrate organisational data, such as engineering blueprints, trade secrets, recipes, intellectual property, or process telemetry. Configure DLP systems to obstruct the transmission of information through various corporate resources, including email, web channels, and physical media like USB drives. DLP capabilities can be integrated into security products like firewalls or utilised as standalone suites through network and host-based agents (The MITRE Corporation, 2023b).
- **Organisational** – Depending on the organisation's size, number of assets, number of devices containing sensitive information and risk appetite as discussed in Section 6.3, this would shape the scope of the DLP deployment.
- **Procedural** – Develop policies, standards, and procedures (as discussed in Section 6.7.3.4) that cover the DLP system implementation discussed under technological factors.
- **People** – Provide training to security staff dealing with DLP, ensuring they can implement, configure, and monitor the system.

6.8 Recommendations

To adequately protect an IIoT environment in the transportation sector of South Africa, the controls should be implemented as per the phases discussed in Section 6.7.3, starting with the current state assessment, executive buy-in and strategy.

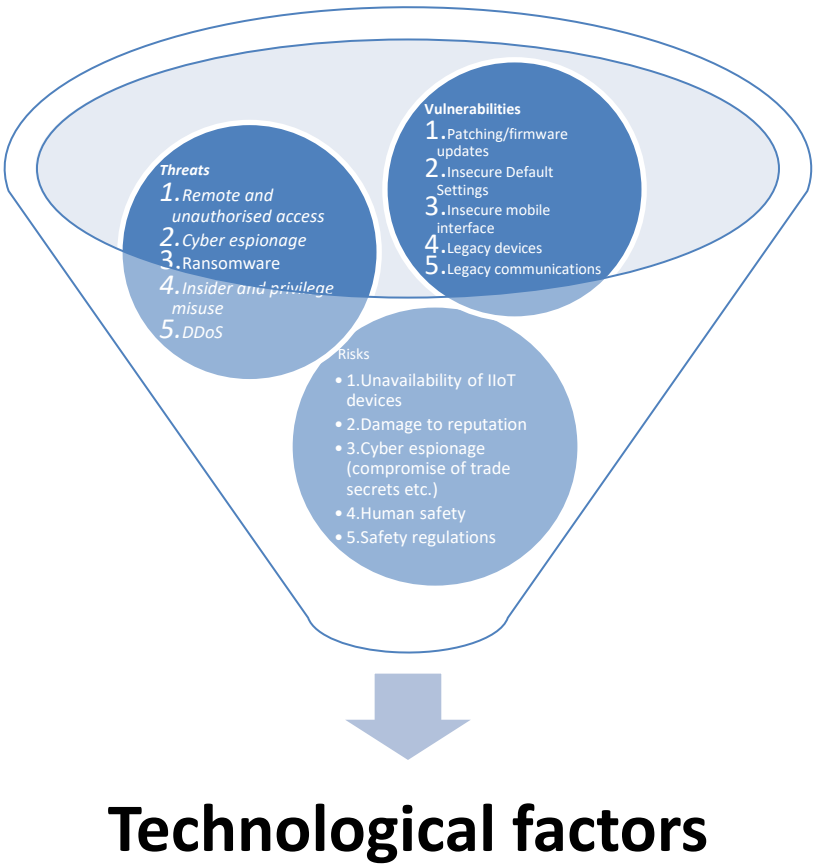


Figure 6-19: Technology factors visualised

6.8.1 Technological factors (Threats)

6.8.1.1 Remote Access and Unauthorised Access

To effectively protect the IIoT environment against remote access and unauthorised access, access to IIoT systems should be restricted, and remote access be managed and regularly reviewed. Appropriate authentication mechanisms (e.g., strong authentication) with encryption should be implemented for all remote connections. Use Virtual Private Networks (VPNs) or secure remote access gateways to establish secure connections. Security reviews of all third parties having remote access to the IIoT are performed and managed regularly.

6.8.1.2 Cyber Espionage

Cyber espionage is one of the top three threats to IIoT in the transport sector of South Africa, which is unique in that it is not one of the top threats to general IIoT. To mitigate cyber espionage, regular system monitoring of the IIoT environment should be performed. This includes network traffic and user access (including remote access) to detect suspicious behaviour, indicators of compromise, and

anomalies, to detect and block sophisticated attacks. At a minimum, Audit logs should be enabled and reviewed to monitor access and remote access activities for suspicious behaviour or unauthorised access. Critical and confidential data of the IIoT environment, whether stored in a database, Operating System, Application, or device, should be appropriately encrypted, and regularly monitored and reviewed. Encrypt sensitive data stored on mobile devices and implement robust authentication mechanisms. Ensure that critical and confidential communication to and from IIoT systems and devices, whether wired or wireless, are appropriately encrypted and are regularly monitored and reviewed.

6.8.1.3 Malware (particularly ransomware)

Implementing vendor-accredited and configured anti-malware software would mitigate malware such as ransomware for the IIoT environment is protected against malware and external threats by. In cases where anti-malware software cannot be installed, alternative protective measures should be adopted, such as performing gateway anti-virus scanning or conducting manual checks on media.

6.8.1.4 Insider and Privilege Misuse

To mitigate insider and privilege misuse, access to IIoT systems should be restricted and regularly reviewed. Regular system monitoring of the IIoT environment should be performed. This includes network traffic and user access (including remote access) to detect suspicious behaviour, indicators of compromise, and anomalies, to detect and block sophisticated attacks. At a minimum, Audit logs should be enabled and reviewed to monitor access and remote access activities for suspicious behaviour or unauthorised access. Also ensure that changes to the IIoT systems are managed, and all data conversions are formally managed per the System Development Lifecycle Methodology and Change and Release Management Procedure.

6.8.1.5 Distributed Denial of Service (DDoS)

To ensure that IIoT environment is protected against DDoS attacks, it should be segregated from other networks by appropriately installed, configured, and managed layer seven firewalls. Implementing Web application firewalls (WAF) would assist in protection against DDoS attacks and other web application attacks. Where firewalls are costly, segmentation can be achieved via network subnets with unique security controls and protocols.

Redundancy should exist for critical IIoT environments, systems, equipment, and components. These include redundant networks, switches, servers, workstations, and devices. Implement redundancy and failover mechanisms to maintain service availability during example, a DDoS attack.

A Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) should be developed in cooperation with business process owners and based on a risk-based approach and should clearly define the roles and responsibilities of the recovery team members. The DRP and BCP should be tested

and kept up to date to ensure recovery of IIoT systems to minimise business impact in the event of a significant disruption such as a DDoS attack.

6.8.2 Technological factors (Vulnerabilities)

6.8.2.1 No or delay in Patching or Firmware Updates

To mitigate the vulnerability of no or delay in patching and firmware updates, ensure a formal patch management process is in place to allow timely and regular updates for all IIoT devices and systems. Thoroughly test all patches on a testbed before installing them on production systems and, where possible, automate patch management systems to streamline the process and reduce the risk of delays. Where it is not possible or practical to implement patches, alternative appropriate protection measures should be considered. Maintain an inventory of all devices and their firmware versions to track and schedule necessary updates. Ensure patching efforts are prioritised based on regular vulnerability assessments. Regularly update and patch mobile applications to address any security vulnerabilities. Also, establish communication channels with vendors to receive timely notifications about security patches and updates.

6.8.2.2 Insecure Default Settings

To address the vulnerability of insecure default settings, ensure that the IIoT devices and supporting infrastructure have been hardened. Change default passwords and usernames on IIoT devices and systems to strong and unique credentials, implement password policies, security features activated, unused services and ports have been disabled in the operating systems and applications to prevent unauthorised use and to reduce the attack surface. Disable removable media (such as USB drives) where possible. Where removable media is necessary, procedures are in place to ensure these are checked for malware before use. Implement secure configuration practices, such as disabling unnecessary features or protocols. Review and update device configurations to ensure they align with security best practices. Before deployment, perform security assessments on new devices to identify and mitigate any insecure default settings. Ensure that configuration of IIoT systems has been documented in a configuration management database (CMDB). No changes to the IIoT configuration are made without a corresponding CMDB update.

6.8.2.3 Insecure Mobile Interface

To mitigate against insecure mobile interfaces, ensure secure Software Development processes, such as DevSecOps, are implemented. DevSecOps involves incorporating security testing throughout every phase of the software development process. It encompasses tools and procedures that promote cooperation among developers, security experts, and operations teams to develop effective and protected software. Conduct security testing and code reviews for mobile applications to identify and fix vulnerabilities. Implement secure coding practices for mobile applications interacting with IIoT

devices. Implement digital signatures to verify the authenticity of application DLLs before they are executed.

6.8.2.4 Legacy Endpoints and Devices

Identify all legacy endpoints and devices via a comprehensive asset register that contains all IIoT assets. Maintain an inventory of all devices and their firmware versions to track and schedule necessary updates and replacements. Assess the risks associated with legacy endpoints/devices in the IIoT environment and develop a plan to phase out or upgrade legacy devices to more secure and modern alternatives.

6.8.2.5 Legacy Communications and Protocols

Using secure communication protocols (e.g., HTTPS) for data transmission to and from IIoT devices will mitigate the vulnerability of legacy communication and protocols. Identify and assess the risks associated with legacy communications and protocols used in the IIoT environment. Where feasible, transition to more secure communication protocols, such as TLS or secure VPNs. Disable or restrict the use of insecure protocols or implement additional security measures (e.g., encryption, authentication) for legacy protocols. Regularly review and update protocols to ensure security standards and best practices compliance. Implement network monitoring and intrusion detection systems to detect and block all malicious activities targeting legacy communications. Ensure that wireless networks are minimised, and wireless connections are regularly monitored and reviewed.

6.8.3 Technological Factors (Risks)

6.8.3.1 Unavailability of IIoT Devices or Networks

To effectively mitigate the risk of the unavailability of IIoT devices or networks, ensure redundancy exists for critical IIoT environments, systems, equipment, and components. These include redundant networks, switches, servers, workstations, and devices. Implement redundancy and failover mechanisms to maintain service availability during example, a DDoS attack. Ensure that adequate backups and recovery procedures are in place to safeguard critical data and that the integrity of backups is regularly tested.

A Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) should be developed in cooperation with business process owners and based on a risk-based approach and should clearly define the roles and responsibilities of the recovery team members. The DRP and BCP should be tested and kept up to date to ensure recovery of IIoT systems to minimise business impact in the event of a significant disruption such as a DDoS attack.

6.8.3.2 Damage to Reputation

This risk could be due to various things, e.g. unavailability of IIoT devices, cyberattacks or breaches. To fully mitigate this, the cybersecurity framework discussed in Section 6.7.3 should be implemented and monitored.

6.8.3.3 Cyber Espionage Resulting in the Compromise of Trade Secrets, Research and Development, and other Sensitive Information

To mitigate the risk of cyber espionage, regular system monitoring of the IIoT environment should be performed. This includes network traffic and user access (including remote access) to detect suspicious behaviour, indicators of compromise, and anomalies, to detect and block sophisticated attacks. At a minimum, Audit logs should be enabled and reviewed to monitor access and remote access activities for suspicious behaviour or unauthorised access. Critical and confidential data of the IIoT environment, whether stored in a database, Operating System, Application, or device, should be appropriately encrypted, and regularly monitored and reviewed. Encrypt sensitive data stored on mobile devices and implement robust authentication mechanisms. Ensure that critical and confidential communication to and from IIoT systems and devices, whether wired or wireless, are appropriately encrypted and are regularly monitored and reviewed.

6.8.3.4 Human Safety

To ensure human safety, adequate physical security measures should be implemented to restrict access to areas housing IIoT equipment and devices. Improve physical security by implementing access control systems, surveillance cameras, and security guards at critical locations. Establish strict access control policies and procedures to restrict physical access to IIoT devices and infrastructure. Conduct regular inspections and maintenance of physical security measures to ensure their effectiveness. Implement tamper-evident seals or locks to identify and deter physical tampering attempts.

Ensure a resilient infrastructure with necessary facilities is installed to protect the IIoT systems. Equipment should reside in environmentally controlled areas at appropriate ambient conditions to ensure proper and sustainable operation.

6.8.3.5 Safety Regulations, Considerations, Consequences, and Implications

To ensure compliance against safety regulation, consideration, consequence, and implications, implement the controls listed in Section 7.3.3.4.

6.8.4 Organisational Factors

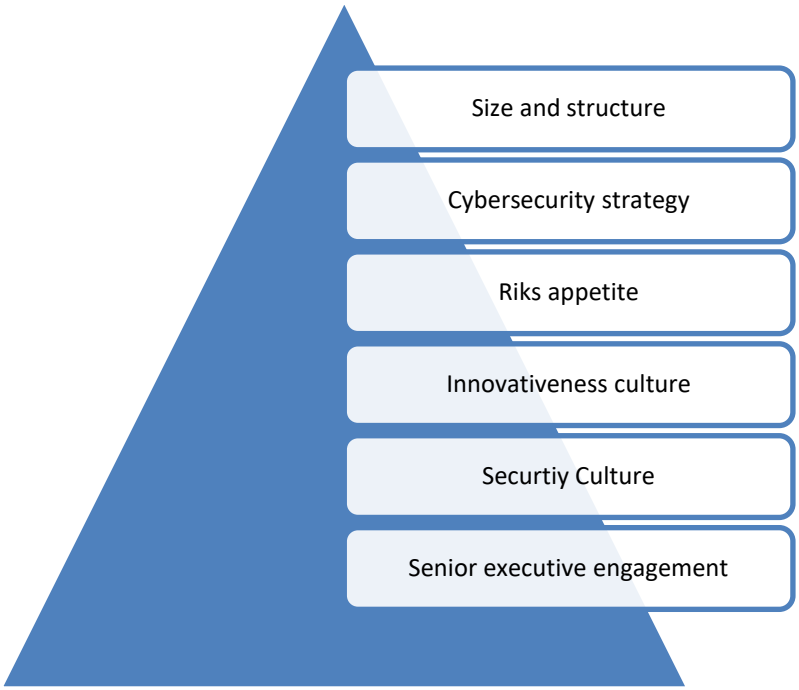


Figure 6-20: Organisational Factors visualised

6.8.4.1 Size and Structure

Ensure an adequate structure with skilled cybersecurity professionals to support IIoT. When assessing the size and composition of the IIoT security team, take into account the following factors: number of IIoT devices deployed, industry type (e.g. the security needs of a transportation fleet management system may differ from those of a smart traffic management system), involvement of multiple organisations/divisions, and the security posture of the organisation.

6.8.4.2 Cybersecurity Strategy

Develop a cybersecurity strategy by ensuring the IIoT security and organisational strategies are aligned. Key elements to consider for this control include:

- Define a clear and well-defined security model that outlines the organisation's approach to securing IIoT systems in the transport sector.
- Assess and improve the organisation's current security posture concerning IIoT.
- Clearly define the security objectives the organisation aims to achieve for its IIoT environment.

Conduct a thorough assessment of security risks associated with IIoT and identify and evaluate potential risks, considering data privacy, device vulnerabilities, network security, and operational risks. Develop a comprehensive threat model specific to the IIoT environment by identifying potential threats, their likelihood, impact, and potential attack vectors. Incorporate internal and external threats

into the cybersecurity roadmap/strategy, aligning it with the threat model. This will help establish proactive measures that effectively address the identified threats.

6.8.4.3 Risk Appetite

To enhance the maturity of risk management practices and establish a proactive approach to addressing the risks associated with IIoT technologies in the transport sector. Develop a well-defined risk management strategy that encompasses the unique challenges and requirements of IIoT environments. This strategy should outline the organisation's methodology for managing risks, including risk appetite, risk acceptance criteria, outsourcing of risk, risk avoidance, risk transfer or mitigation, and risk tolerance levels specific to IIoT.

6.8.4.4 Innovativeness Culture

Establish an innovation enablement program that fosters an innovative culture within the organisation and promotes adopting innovative practices specific to IIoT security. Create platforms and channels facilitating employee collaboration and sharing expertise and experiences regarding IIoT. This can include forums, workshops, or innovation hubs where employees can brainstorm ideas, exchange knowledge, and work together to find innovative solutions for securing IIoT systems.

6.8.4.5 Security Culture

Promote a culture of accountability and responsibility by clearly defining roles and responsibilities related to IIoT security. This includes raising awareness about potential threats, best practices for securing IIoT devices, the impact of individual actions on overall security and conducting situational awareness programs to educate employees on recognising and responding to security incidents or reporting suspicious activities related to IIoT. Encourage employees to actively engage in security discussions and provide feedback or suggestions to improve IIoT security practices.

6.8.4.6 Senior Executive Engagement with Security

To establish a program for executive management to enhance the understanding and involvement of senior executives in IIoT security. Key factors to consider include:

Effective and Clear Communication: Develop a communication strategy communicating the importance of IIoT security to senior executives. Clearly articulate the potential risks, business impacts, and strategic implications of inadequate security measures. Use concise and relevant language to convey the message and emphasise the role of senior executives in driving a strong security posture.

Security Metrics and Effectiveness:

- Implement security metrics that provide insights into the effectiveness of IIoT security measures.

- Establish key performance indicators (KPIs) that align with business objectives and enable senior executives to assess the organisation's security posture.
- Regularly report these metrics to senior executives, highlighting areas of improvement, emerging threats, and the effectiveness of security initiatives.

Stakeholder Expectations and Business Decision Makers: Foster an understanding of stakeholder expectations related to IIoT security among senior executives. Enable executives to make informed business decisions with the necessary information and insights. This includes involving senior executives in risk assessment, presenting risk scenarios, and discussing potential mitigation strategies.

Effective Business Decisions:

- Encourage senior executives to prioritise IIoT security in decision-making processes.
- Incorporate security considerations into strategic planning, budget, and resource allocation decisions.
- Promote a culture where security is seen as a critical enabler of business objectives and senior executives actively champion security initiatives.

Security Evangelists: Identify and empower security evangelists among senior executives who can advocate for IIoT security within the organisation. These individuals can be role models, sharing their knowledge and experiences to inspire others to prioritise security. Encourage senior executives to actively participate in industry forums, conferences, and thought leadership events to stay updated on emerging security trends and technologies.

6.8.5 Procedural Factors

Figure 6-21: Procedural factors visualised

6.8.5.1 Security Incident Response

Ensure that response capabilities to IIoT system incidents are understood and managed. These include a helpdesk system to prioritise and track incidents and escalation of long outstanding incidents. Procedures should be in place to escalate an incident to a disaster and revert to BCP or DRP should it be required. This will improve the maturity of the organisational incident response plan and ensure it adequately addresses the risks associated with IIoT technologies in the transport sector of South Africa. Consider the following factors when enhancing the incident response plan:

Implement comprehensive monitoring and analysis techniques specific to IIoT environments. This includes rule-based analysis, forensic analysis, root cause analysis, behavioural analysis, and monitoring of encrypted channels. Incorporate these techniques into the incident response plan to enable effective detection, analysis, and response to security incidents involving IIoT systems.

Conduct periodic testing and evaluation of the incident response plan's effectiveness using tabletop exercises, simulations, and drills to ensure readiness in responding to incidents. Identify gaps and areas of improvement and update the plan, given that. Monitor emerging IIoT threats and adapt the incident response procedures to address new risks and vulnerabilities as they arise.

6.8.5.2 Risk Management

To enhance the maturity of risk management practices and establish a proactive approach to addressing the risks associated with IIoT technologies in the transport sector. Develop a well-defined risk management strategy that encompasses the unique challenges and requirements of IIoT environments. This strategy should outline the organisation's methodology for managing risks, including risk appetite, risk acceptance criteria, outsourcing of risk, risk avoidance, risk transfer or mitigation, and risk tolerance levels specific to IIoT.

Develop a robust threat model specific to the IIoT environment to identify and analyse potential threats, and threat actors, understand their motivation, capabilities, likelihood, and impact, and map them to the organisation's risk appetite. Implement effective threat mitigation measures to align with the organisation's risk appetite. This includes implementing security controls, conducting regular vulnerability assessments and penetration testing, and leveraging threat intelligence to identify and mitigate emerging threats proactively. Ensure mitigation efforts are prioritised based on risk severity and aligned with the organisation's risk appetite. Regularly reassess the organisation's risk appetite considering new threats and adjust risk management strategies accordingly.

6.8.5.3 IT Governance and Compliance

Establish a complete Information Security Management System (ISMS) for IIoT encompassing policies, procedures, and standards. Define clear roles and responsibilities for IIoT governance and ensure alignment with overall organisational governance structures. Develop and communicate

security policies covering all IIoT security and governance areas. Implement robust configuration management standards for IIoT devices and systems and enforce secure configuration practices to minimise vulnerabilities and ensure consistency across IIoT deployments.

Ensure a compliance plan is in place for legal and regulatory requirements. Ensure that the IIoT environment adheres to relevant privacy regulations, such as the POPIA (Government of Republic of South Africa, 2013), King IV (Institute of Directors in Southern Africa, 2009) and ECTA (Government of Republic of South Africa, 2002a), and RICA (Government of Republic of South Africa, 2002b) in South Africa. Ensure compliance with IT (Information Technology) and OT (Operational Technology) regulations that govern the use and integration of IIoT systems and adherence to Safety Regulations. All mobile-enabled systems (GSM) must conform to the RICA Act.

6.8.5.4 Policies, Standards, and Procedures

To ensure adequate policies, standards and procedures are implemented and communicated to all relevant stakeholders to govern the IIoT environment. Identify and understand the relevant regulatory and compliance requirements specific to IIoT in the transport sector and develop processes and controls to ensure compliance with these regulations and methods for monitoring and reporting compliance status.

Establish a complete policies, procedures, and standards for IIoT security. Define clear roles and responsibilities for IIoT governance and ensure alignment with overall organisational governance structures. Develop and communicate security policies covering all IIoT security and governance areas. Implement robust configuration management standards for IIoT devices and systems and enforce secure configuration practices to minimise vulnerabilities and ensure consistency across IIoT deployments.

Ensure mechanisms are in place to monitor and report assurance activities to assess the effectiveness of governance processes for IIoT. This could include regular internal and external audits, compliance monitoring, vulnerability assessments, and penetration testing of IIoT systems. Develop metrics and key performance indicators (KPIs) to measure the effectiveness of governance controls and continuously improve the security posture of IIoT.

6.8.5.5 Legal and Regulatory Requirements

Ensure a compliance plan is in place for legal and regulatory requirements. Ensure that the IIoT environment adheres to relevant privacy regulations, such as the POPIA (Government of Republic of South Africa, 2013), King IV (Institute of Directors in Southern Africa, 2009) and ECTA (Government of Republic of South Africa, 2002a), and RICA (Government of Republic of South Africa, 2002b) in South Africa. Ensure compliance with IT (Information Technology) and OT

(Operational Technology) regulations that govern the use and integration of IIoT systems and adherence to Safety Regulations. All mobile-enabled systems (GSM) must conform to the RICA Act.

6.8.6 People Factors

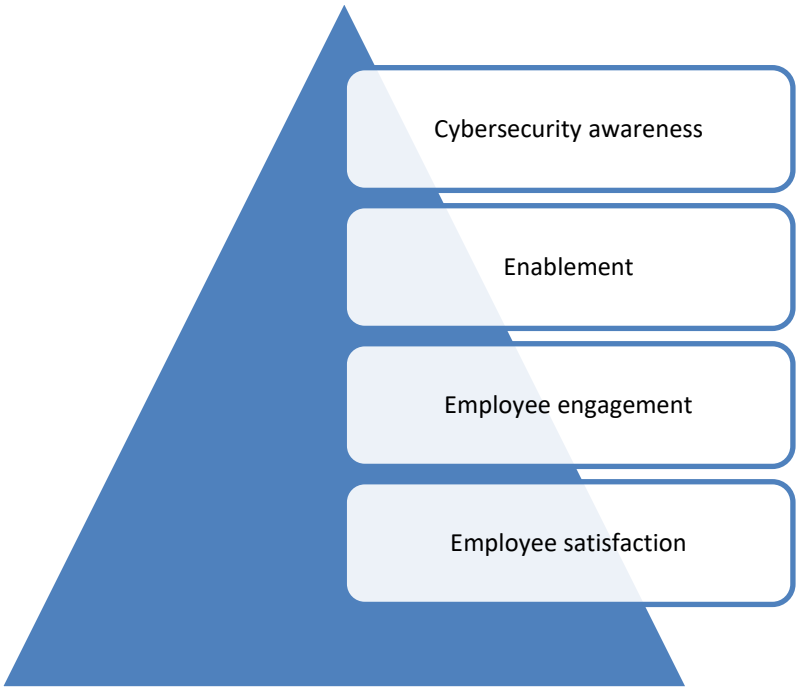


Figure 6-22: People factors visualised

6.8.6.1 Cybersecurity Awareness

To enhance awareness and skills, it is crucial to conduct continuous and comprehensive security training and educational programs for all employees. These programs should emphasise the significance of security awareness, specifically for IIoT environments. This includes raising awareness about potential threats, best practices for securing IIoT devices, the impact of individual actions on overall security and conducting situational awareness programs to educate employees on recognising and responding to security incidents or reporting suspicious activities related to IIoT. Promote a culture of accountability and responsibility by clearly defining roles and responsibilities related to IIoT security.

Establish regular communication channels to disseminate security-related information, updates, and best practices to all stakeholders. This can be done through newsletters, internal bulletins, or online platforms. Encourage employees to actively engage in security discussions and provide feedback or suggestions to improve IIoT security practices. Regularly assess the effectiveness of the security awareness program and seek feedback from employees. Use this feedback to improve the program and address any gaps identified. Conduct regular phishing simulations to identify users who fell victim to these and provide additional training for them.

6.8.6.2 Enablement

Establish cybersecurity training programs that range from general employees to IIoT security professionals. This will minimise human error and increase investment in expertise. The training programs for employees should focus on general security skills highlighting the importance of security, risk management, and incident response. Develop specialised training programs that focus specifically on IIoT security. Establish a culture of continuous learning and professional development by encouraging employees to pursue certifications, attend industry conferences, and participate in workshops and webinars related to general security and IIoT security. Continuously evaluate the effectiveness of the training programs and make necessary improvements.

6.8.6.3 Employee Engagement

Ensure an employee engagement program is developed to establish communication channels and build relationships between engineering/OT and security staff, IT and security staff, management and security staff and executive engagement with security staff. The program should additionally deliver training and promote awareness, integrating security considerations into workflows and decision-making processes. It should cultivate a culture that prioritises security awareness and fosters a sense of accountability. Include security metrics and reporting mechanisms in management KPIs to provide security posture and progress visibility. Encourage regular meetings and discussions between management and security staff to review security strategies, initiatives, and risk mitigation plans. Arrange periodic executive briefings and presentations by security staff to provide insights into emerging security threats, industry trends, and the organisation's security posture. Provide executive management with regular reports on the effectiveness of security controls and risk management efforts.

6.8.6.4 Employee Satisfaction

Implement employee recognition and reward programs to acknowledge and incentive exceptional performance, fostering a positive work environment and job satisfaction. This should also include an effective communication strategy to address employee concerns and provide regular updates on organisational goals, strategies, and progress. Establish channels for employees to provide feedback, suggestions and express concerns about their work environment, job satisfaction, and IIoT security. Conduct employee satisfaction surveys periodically to gather insights and identify areas for improvement. Implement employee recognition programs to acknowledge and reward exceptional performance, fostering a positive work environment and job satisfaction.

Invest in robust, user-friendly tools and technologies that effectively enable employees to manage IIoT security. Provide comprehensive training and support to employees on adequately using these tools and technologies. Regularly assess the effectiveness and usability of the tools and make necessary improvements based on employee feedback.

Implement policies and practices that promote work-life balance and employee well-being. Offer avenues for professional development and advancement to boost employee motivation and engagement. Foster a positive work environment encouraging collaboration, open communication, and teamwork. Ensure that employees have the necessary resources, training, and support to perform their roles effectively in the IIoT environment. Regularly assess employee workload and adjust to prevent burnout and optimise productivity.

6.9 Summary

This chapter discussed the impact of the technological, organisational, procedural and people factors for IIoT security on the SA transport sector.

The technological factors influencing IIoT cybersecurity in the SA transport sector are existing and new threats due to IIoT, vulnerabilities, and risks. The organisational factors Influencing IIoT cybersecurity in the SA transport sector are size and structure, cybersecurity strategy, risk appetite, innovativeness culture, security culture, and senior executive engagement with security. The procedural factors that influence IIoT cybersecurity in the SA transport sector are security incident response, risk management, IT governance and compliance, policies, standards and procedures and legal and regulatory requirements. The people factor that influence IIoT cybersecurity in the SA transport sector are cybersecurity awareness, enablement, employee engagement and employee satisfaction. The correlation between technological, organisational, procedural, and people factors in IIoT cybersecurity for the SA transport was discussed.

A cybersecurity framework consisting of security controls is developed using the data collected to address the technological, organisational, procedural and people factors influencing IIoT cybersecurity in the SA transport sector. These mitigate the threats, vulnerabilities, and risks of IIoT cybersecurity in the transportation sector of South Africa. Priority is given to controls that mitigate the existing and new threats due to IIoT, vulnerabilities and risks. The cybersecurity framework is reviewed and validated against the MITRE ATT&CK framework for ICS. The addition of appropriate controls addressed the gaps identified. A list of recommendations per factor are provided. The next chapter concludes the study and suggests future work.

Chapter 7 Conclusions and Recommendations

7.1 Introduction

The previous chapter interpreted and discussed the results of the data analysis using the online questionnaire and secondary data analysis. This chapter concludes the study and examines whether the research objectives are achieved. This thesis consisted of seven chapters (including this chapter).

Chapter 1 introduced the study and described the research approach. The study aims to assess the factors (technological, organisational, procedural and people) influencing IIoT cybersecurity in the SA transport sector and to develop and validate a cybersecurity framework for IIoT in the SA transport sector using the data collected. Chapter 2 presented a literature review on IIoT. Chapter 3 discussed the research methodology and the research design that guided this study, while Chapter 4 presented the primary data and used quantitative data analysis. Chapter 5 presented the secondary data and used qualitative data analysis. Chapter 6 presented a discussion based on the primary and secondary data.

This chapter concludes the study by presenting the conclusions, the limitations, proposes areas for future research and a conclusion. Figure 7.1 is a graphical representation of the outline of this chapter and its overall structure.

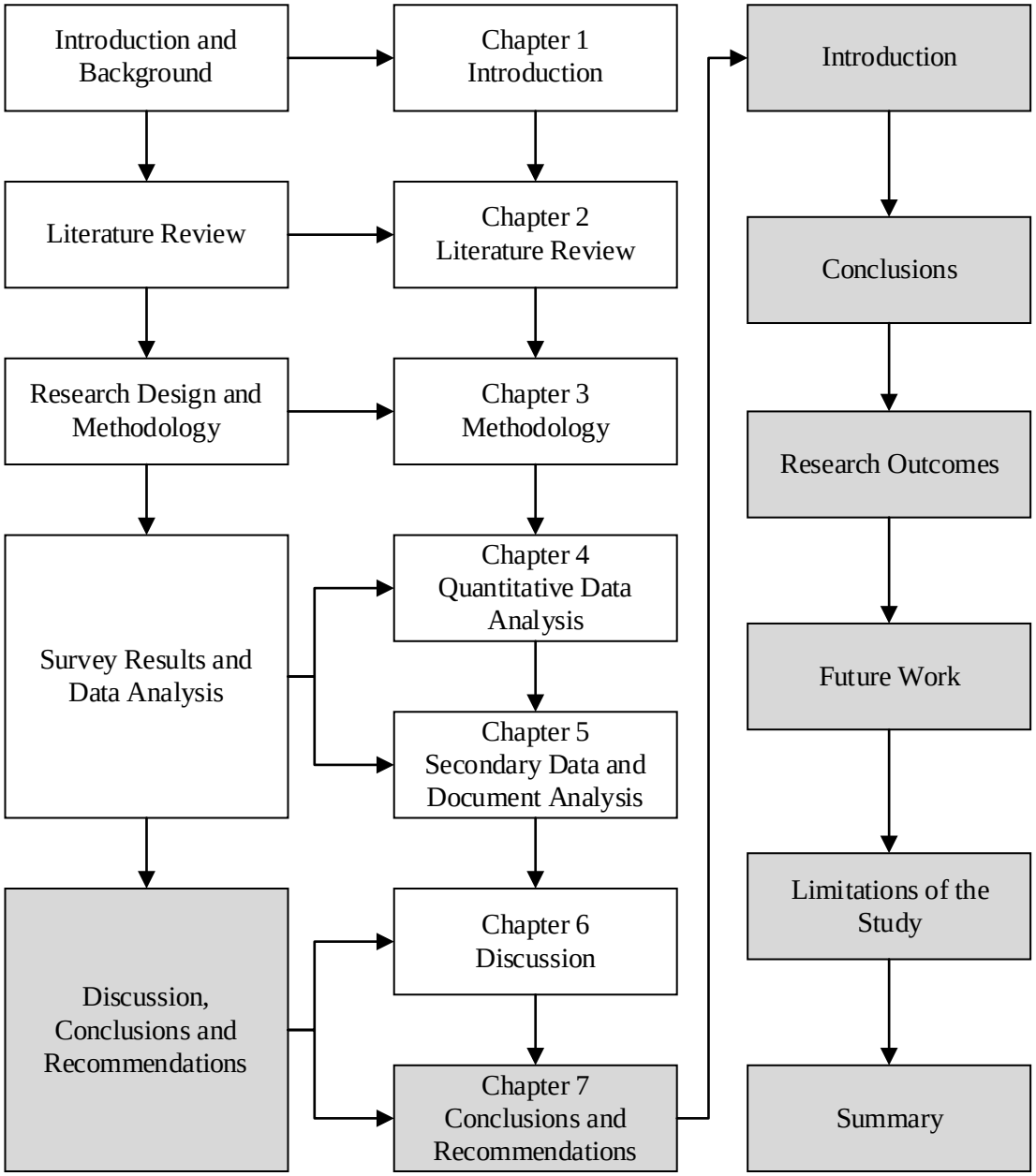


Figure 7-1: Graphical representation of Chapter 7 outline

7.2 Conclusions

The research objectives are met and are discussed further in the section below.

7.2.1 Research Objective 1 – To determine the extent to which the Technological Factors Influence IIoT Cybersecurity in the South African Transport Sector

The study found that the technological factors existing and new threats due to IIoT influencing IIoT cybersecurity in the SA transport sector are remote access, cyber espionage, malware (particularly ransomware), insider and privilege misuse, and Distributed Denial of Service (DDoS). Cyber espionage is a unique IIoT threat in the SA transport sector compared to general IIoT threats. Section 6.2.1 discussed the extent to which existing and new threats impact the transport sector. One such

example is the significant disruptions experienced after a ransomware attack on Transnet in 2021, severely impacting the South African economy.

The vulnerability factors influencing IIoT cybersecurity in the SA transport sector are no or delay in patching or firmware updates, insecure default settings, insecure mobile interface, legacy endpoints or devices, and legacy communications/protocols. Section 6.2.2 discusses the extent to which vulnerabilities impact the transport sector; examples include exploitation by cyber threats and jeopardizing operational continuity and system integrity.

The risk factors influencing IIoT cybersecurity in the SA transport sector are the unavailability of IIoT devices or networks, damage to reputation, cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information, human safety, and safety regulations/considerations/consequences/implications. Section 6.2.3 presents a comprehensive discussion of risks' impact on the transport sector. Risks can lead to service interruptions, delays, safety concerns, economic losses, reduced competitiveness, and even a threat to national security. It is of the utmost importance to evaluate and manage these IIoT risks effectively to ensure the safety and efficiency of the transport sector in SA.

The top risks, such as cyber espionage, match the top threats. Comparing this with the secondary data analysis, it coincides with the top threats found by the study showing consistency in the results. The top vulnerabilities also match the OWASP serious vulnerabilities discussed in Chapter 2. These factors could cause the unavailability of IIoT devices and lead to direct financial loss or physical asset damage.

7.2.2 Research Objective 2 – To critically assess the Organisational Factors Influencing IIoT Cybersecurity in the South African Transport Sector

The study assessed the organisational factors (Size and structure, Cybersecurity strategy, Risk appetite, Innovativeness culture, Security culture, and Senior executive engagement with security) influencing IIoT cybersecurity in the SA transport sector.

The number of staff supporting IIoT in the transport sector of SA is limited with an even more constrained number dedicated to security roles and IIoT security roles.

The size and structure of IIoT security staff are determined by the number of devices, the system industry, and the involvement of multiple organisations. They are influenced by resource availability, groups or individuals that control or influence, and the organisation’s security posture.

The maturity of the cybersecurity roadmap/strategy supporting IIoT in the transport sector of SA is managed and not defined or quantitatively managed as per desired state. The cybersecurity roadmap/strategy of IIoT is determined by the security model, security posture, security objective, security risks, threat model, and Cybersecurity Capability Maturity model and influenced by business

decisions, business needs, business objectives and risk strategy, business priorities, business sectors and verticals risk appetite of the organisation.

The maturity of the risk appetite for the IIoT environment in the transport sector of SA is managed and not defined or quantitatively managed as per the desired state. The risk appetite of IIoT is determined by the risk strategy (e.g. risk avoidance, risk acceptance, outsourcing of risk, risk transfer and risk mitigation), threat model/modelling, threat mitigation, threat actors, threat identification, and impact of unavoidable threat and influenced by replacement cost, cost of an incident/consequence; mitigation exceeds the cost, balance of cost, cost of upgrading security, and cost versus effectiveness of security controls, business risk/risks, business objectives, business priorities and business sectors.

The maturity of the innovativeness culture supporting IIoT for IIoT environment in the transport sector of SA is managed and not defined or quantitatively managed as per desired state. The innovativeness culture of IIoT is influenced by Evolving data analytics techniques, evolving landscape of endpoint and communication, use of technologies and use of expertise, Evolution in both business and implementation, use of expertise to make their IIoT systems trustworthy, evolving data analytics techniques, and Technologies for creating a trustworthy system.

The maturity level of the security culture that supports IIoT in South Africa's transportation sector is currently managed. It needs to be clearly defined and quantitatively managed to achieve a more mature state. The security culture of IIoT is influenced by security-aware culture, instil awareness, situational awareness, adequate awareness and awareness of accountability and responsibility, security evangelists, difficulty applying security, security posture of the organisation and security is overlooked or less critical in OT, different cultures (OT and IT), and different priorities, convergence of IT and OT, situational awareness of IoT ecosystem and IoT security, Constantly train, train end users, and train staff, understand characteristics of IoT affect managing cybersecurity, and understand the use of IoT.

The maturity of Senior/Executive understanding of IIoT security risks for IIoT environment in the transport sector of SA is managed. It needs to be defined and quantitatively managed as per the desired state. The Senior executive engagement with security for IIoT is determined by effective and clear communication, security metric and effectiveness, stakeholder expectation and business decision-makers and influenced by effective business decisions, security evangelists, security programs, security risks, accurate representation of security, and business communication.

The extent to which these factors impact the transport sector is discussed in Section 6.3.

7.2.3 Research Objective 3 – To critically assess the Procedural Factors Influencing IIoT Cybersecurity in the South African Transport Sector

The study assessed the procedural factors (Security incident response, Risk management, IT governance and compliance, Policies, standards and procedures and Legal and regulatory requirements) influencing IIoT cybersecurity in the SA transport sector.

The maturity of the organisational incident response plan for the IIoT environment in the transport sector of SA is between managed and defined and not quantitatively managed as per desired state. The Incident response plan to address IIoT environment risk is below managed and not at the desired state of quantitatively managed. It indicates that although organisations have an incident response plan between managed and defined, it does not address the IIoT risk sufficiently.

The organisational incident response plan for IIoT is influenced by monitoring and analysis such as rule-based analysis, forensic analysis, root cause analysis, behavioural analysis, and monitoring of encrypted channels, captures, and data. Incident response plans, rapid response, consumer notification plans, identification and detection of security violations, controls, and configurations also influence it.

The maturity of risk management supporting IIoT for IIoT environment in the transport sector of SA is managed, and far below the desired state of quantitatively managed where processes are measured and controlled. The organisational risk management for IIoT is influenced by risk assessments, risk avoidance, risk analysis, risk strategy, transferring of risk, residual risk, quantitative risk, risk considerations, risk mitigation, risk models and risk acceptance.

The maturity of Governance processes for IIoT in the transport sector of SA Is managed and not defined or quantitatively managed as per the desired state. The IT governance and compliance of IIoT is determined by regulatory and compliance requirements, security program and security policies, security configuration management, assurance, audit, compliance requirements, and efficient systems management.

The maturity of general security policies/procedures implemented for an IIoT environment in the transport sector of SA is between managed and defined, while the IIoT security policies/procedures/controls implemented, the maturity of Governance processes for IIoT and the maturity of Control framework for IIoT in the transport sector of SA is all strongly leaning towards managed and not defined or quantitatively managed as per desired state. The top three frameworks used by the respondents to govern and secure their IIoT environments in the transport sector of SA are COBIT, secondly ISO 27001 series and NIST. The implementation of general security policies/procedures is more mature than the maturity of the IIoT security policies/procedures/controls implemented, of which ISO 27001 or NIST might be more suitable.

The Policies, standards and procedures for IT governance and compliance of IIoT are determined by security policies, security models, security objectives, security controls, security frameworks and other policies (e.g., data retention policy, password policy, organisational policy, data protection policy, endpoint protection).

The legal and regulatory requirements for an IIoT environment in the transport sector of SA are one of the top three (3) priorities. Privacy regulations, security regulations, IT and OT regulations, safety regulations, regulatory policy, changes, and directives from regulatory policy determine the legal and regulatory requirements of IIoT.

The extent to which these factors impact the transport sector is discussed in Section 6.4.

7.2.4 Research Objective 4 – To critically assess the People Factors Influencing IIoT Cybersecurity in the South African Transport Sector

This study assessed the people factors (Cybersecurity awareness, Enablement, Employee Engagement and Employee satisfaction) influencing IIoT cybersecurity in the SA transport sector.

The maturity of Security awareness for an organisation with IIoT devices in the transport sector of SA is between managed and defined and not quantitatively managed as per desired state. The maturity of security awareness specific to IIoT in the transport sector of SA is below managed and far from quantitatively managed as per the desired state. The security awareness of IIoT is influenced by situational awareness, security-aware culture, maximising user awareness, awareness of IoT security, and constant training of staff and users.

The maturity of employees that have general security skills in an IIoT environment in the transport sector of SA is managed. The maturity of the organisation enabling staff for security in an IIoT environment in the transport sector of SA is below managed and far from the desired state of quantitatively managed. There is a clear gap in general security skills; organisations must address this by enabling staff.

The maturity of employees that have IIoT security skills in an IIoT environment in the transport sector of SA is even less mature between initial and managed. Looking at the maturity of Employees being sufficiently trained to deal with IIoT security in an IIoT environment in the transport sector of SA is between initial and managed and not quantitatively managed as per desired state. There is an even more significant gap in IIoT security skills, and organisations address this even less than general security skills by not adequately enabling staff.

The enablement of IIoT is influenced by training staff and users, constantly providing training, the cost of training, building up expertise and using it, and minimising human error.

The maturity of engineering/OT engagement with security staff, the maturity of IT engagement with security staff, the maturity of management engagement with security staff and the maturity of executive management engagement with security staff for IIoT environment in the transport sector of SA are all below managed and not quantitatively managed as per desired state. It indicates a general lack of employee engagement with security staff in the transport sector of SA on all levels, from engineering staff, OT staff, IT staff, management, and executive management.

The employee engagement of IIoT is influenced by end-user communications, in-app notifications communications, enablement of the consumer, consumer notifications, and unauthorised tracking of people's behaviours, activities, and locations.

The maturity of employee satisfaction within an organisation having an IIoT environment in the transportation sector of SA is below managed and not quantitatively managed as per desired state. The maturity of the organisation providing the tools to manage IIoT security in the transportation sector of SA is between initial and managed and below the desired state of quantitatively managed. The maturity of employees' energy and employee productivity are both below managed. This indicates that employees in an IIoT environment in the transport sector of SA are not satisfied, which could be related to the failure of the organisation to provide tools to manage IIoT security, influencing the employee's energy and productivity.

Disclosures influence the employee's satisfaction with IIoT. This reward system gives people initiative, rewarding staff, having a balance consideration of differing motivations, and the level of effort needed to manage.

The extent to which these factors impact the transport sector is discussed in Section 6.5.

7.2.5 Research Objective 5 – To assess the Degree of the Relationships Amongst the BMIS Factors for IIoT Cybersecurity in the South African Transport Sector

The study assessed the people factors (Cybersecurity awareness, Enablement, Employee engagement and Employee satisfaction) influencing IIoT cybersecurity in the SA transport sector.

There is one strong negative correlation between Technological (Threats) and Organisational Factors and a few moderate negative correlations. There is one moderate correlation between the Technological (Vulnerabilities) and Organisational Factors and no strong correlations between Technological (Risks) and Organisational Factors.

There is also a strong negative correlation between Technological (Threats) and procedural factors. By improving security measures and ensuring comprehensive security policies, procedures, and controls, organisations can better protect their physical assets and mitigate the risk of potential damage.

There are moderate positive and negative correlations between Technological (vulnerabilities) and procedural factors. These observations emphasise the importance of addressing vulnerabilities and improving procedural measures to enhance organisations' security posture concerning technological vulnerabilities. There is one moderate correlation between Technological (Risk) and procedural factors.

There are moderate negative correlations between Technological (threats) and people factors and between Technological (vulnerabilities) and people factors. Promoting increased engagement and collaboration between engineering/OT teams and security staff is crucial. There are no strong or moderate correlations between Technological (risk) and people factors.

There are strong correlations between organisational and procedural factors, highlighting the importance of organisational factors, such as cybersecurity strategy, governance processes, culture, and senior executive involvement, in driving the implementation of risk management practices for IIoT.

There is only one strong correlation between the organisational and people factors. This correlation highlights the relationship between organisational factors, such as governance processes, senior executive involvement, and innovative culture, and the level of security awareness specific to IIoT among employees. They indicate that organisations that prioritise risk assessments, have effective governance processes, and promote engagement and collaboration between different teams are likelier to foster a culture of security awareness and knowledge about IIoT security risks among their employees.

There are strong correlations between the procedural and people factors, and they indicate that organisations prioritising these factors are more likely to have a knowledgeable, trained, and prepared workforce to address IIoT security risks and effectively implement security measures.

The extent to which these factors impact the transport sector is discussed in Section 6.6.

7.2.6 Research Objective 6 – To Develop and Validate a Cybersecurity Framework for IIoT in the South African Transport Sector using the Data Collected

The ultimate and final objective is to develop and validate a cybersecurity framework for IIoT in the SA transport sector using the data collected. The process for developing the cybersecurity framework is discussed in Section 6.7.3. A cybersecurity framework for IIoT in the SA transport sector is developed to address the technological, organisational, procedural and people factors influencing IIoT cybersecurity in the SA transport sector. These mitigate the threats, vulnerabilities, and risks of IIoT cybersecurity in the transportation sector of South Africa. The high-level framework is listed in Section 6.7.3 with prevalent controls to implement based on the technological, organisational,

procedural and people factors. The controls are prioritised to focus on and address the top risks, threats and vulnerabilities from the technological factors, and the factors (Organisational, Procedural and People) are used as input into the cybersecurity framework. Priority is given to controls that mitigate the existing and new threats due to IIoT, vulnerabilities and risks. From the cybersecurity framework, the controls are validated against the MITRE ATT&CK Framework for ICS in Section 6.7.4. The addition of appropriate controls addresses the gaps identified.

7.3 Research Outcomes

The research outcome addressed the gap that there is no or limited information available as to the current state of IIoT in South Africa's transport sector, and the factors influencing IIoT security are not known as there are limited studies and research in this area. These include the technological, organisational, procedural and people factors influencing the cybersecurity of IIoT in the transport sector of South Africa. This research identifies and assesses the degree of relationships amongst the factors influencing IIoT cybersecurity in the transport sector of SA to develop and validate a cybersecurity framework aligned with the SA transport sector.

7.3.1 Contribution to Theory

This study created a conceptual model combining the BMIS framework and Design Science Research to aid in developing a cybersecurity framework for IIoT in the transportation sector. The benefit of the model is that it considers various BMIS factors, including technological (threats, vulnerabilities, and risks) and organisational, procedural, and people-related factors, to develop a cybersecurity framework relevant to South Africa's transportation sector. For future work or research, the feasibility and effectiveness of the cybersecurity framework in the industry need to be evaluated.

Another contribution is using the MITRE ATT&CK framework for ICS in Design Science Research to validate the cybersecurity framework. The advantage of validating the cybersecurity framework against the MITRE ATT&CK framework is that it verifies its effectiveness through real-world adversary tactics used by cybercriminals and hackers. This contribution developed a model allowing future researchers to verify their cybersecurity frameworks against the MITRE ATT&CK framework.

7.3.2 Contribution to Global Knowledge

IIoT is a growing area, and since limited research into cybersecurity has been conducted for the transportation sector, there is knowledge sharing because of the study. Parts of the literature on IoT and IIoT, as well as the incidents, threat, vulnerabilities and risks from this study, is published as an academic journal in the *Journal of Information Warfare* in 2020 (Pretorius & Van Niekerk, 2020) and the Proceedings of the *14th International Conference on Cyber Warfare and Security* (ICCWS) on in March 2019 (Pretorius & Van Niekerk, 2019). Parts of the literature on IoT, IIoT and incidents and

the research from the primary data on threats, vulnerabilities, and risks were published in the Journal *Scientia Militaria* in 2023 (Pretorius & Van Niekerk, 2023).

7.3.3 Contribution to Practice

The current state of IIoT in SA and the factors influencing IIoT are assessed as these are unknown. There are limited studies and research in this area. The technological, organisational, and environmental factors influencing the security of IIoT in the SA transport sector are unknown. This research identified and assessed the degree of relationships among the factors influencing IIoT cybersecurity and developed a cybersecurity framework aligned with South African regulations. The control framework will benefit organisations in identifying factors influencing IIoT deployment and help implement controls to mitigate the threats, risks, and vulnerabilities to secure the IIoT devices in their environments.

Science engagement to form awareness around the topic and feedback to professional practice took place as aspects of this study are presented at a practitioner conference, namely at the annual IT Web Security Summit in July 2020 and as an invited presentation to the South African Institute of Electrical Engineers (SAIEE) in March 2019 and CISO Alliance Durban Chapter in July 2019.

7.4 Future Work

From this stage, future work will include a detailed breakdown of the controls, an analysis of the practicality of implementation, and further alignment to South African government legal requirements and international frameworks. Ongoing cybersecurity framework testing in IIoT environments outside of the transport sector will be conducted to ensure the generalisation and applicability of the framework. Repeat studies should also be performed at least every two years to monitor the progress or lack thereof. Step 6 of Design Science Research indicates communication. The final thesis and results must be communicated to stakeholders as part of knowledge production and contribution. Science engagement will raise awareness about the study and provide valuable feedback for professional practice.

According to the research findings in Section 5.9, many Industrial Internet of Things (IIoT) devices in SA are accessible via the Internet. However, the study did not determine whether these devices have any vulnerabilities or which specific sector they belong to. To further explore this issue in future investigations, it may be beneficial to establish a honeypot that imitates an IIoT device to analyse potential weaknesses and attack vectors.

7.5 Limitations of the Study

IIoT security knowledge. An online questionnaire is distributed to organisations in the transportation sector and through professional bodies to solicit responses, and an upfront question is included to

determine the relevance of the respondents. There might be an issue with convenience sampling as the implication would be that other respondents that could have responded have yet to be fully identified.

7.6 Summary

The technological factors influencing IIoT cybersecurity in the SA transport sector are Existing and new threats due to IIoT, Vulnerabilities, and Risks. The top five threats likely to influence IIoT cybersecurity in the SA transport sector are remote access, cyber espionage, malware (particularly ransomware), insider and privilege misuse, and Distributed Denial of Service (DDoS). The top five vulnerabilities likely to influence IIoT cybersecurity in the SA transport sector are no or delay in Patching/firmware updates, insecure default settings, insecure mobile interface, legacy endpoints/devices, and legacy communications/protocols. The top five risks likely to influence IIoT cybersecurity in the SA transport sector are the unavailability of IIoT devices or networks, damage to reputation, cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information, human safety, and safety regulations/considerations/consequences/implications.

The study found that the organisational factors influencing IIoT cybersecurity in the SA transport sector are size and structure, cybersecurity strategy, risk appetite, innovativeness culture, security culture, and senior executive engagement with security. The availability of staff supporting IIoT, especially regarding security, could be improved. The size and structure of IIoT security staff depend on factors such as the number of devices, industry involvement, and resource availability. The maturity of the cybersecurity roadmap/strategy for IIoT in this sector is managed but not clearly defined or quantitatively measured. Similarly, the risk appetite, innovativeness culture, security culture, and senior/executive understanding of IIoT security risks are managed but need a defined and quantifiable state. Various factors influence these aspects, including business decisions, risk strategies, technological advancements, and the convergence of IT and OT. Effective communication, stakeholder engagement, and precise representation of security play a role in senior executive understanding and engagement with IIoT security.

The study found that the procedural factors influencing IIoT cybersecurity in the SA transport sector are security incident response, risk management, IT governance and compliance, policies, standards and procedures and legal and regulatory requirements.

The maturity levels of the incident response plan, risk management, general security policies/procedures, and governance processes for IIoT are between managed and defined and not quantitatively managed as per desired state. The legal and regulatory requirements are one of the top three priorities, and privacy regulations, security regulations, IT and OT regulations, safety regulations, and regulatory policy determine them. Organisations must improve their maturity levels

and implement suitable frameworks to address the cybersecurity risks of their IIoT environment in the transport sector of South Africa.

This study found that the people factors influencing IIoT cybersecurity in the SA transport sector are cybersecurity awareness, enablement, employee engagement and employee satisfaction.

The maturity of security awareness in the IIoT environment of the transportation sector in SA reveals significant gaps in terms of employee engagement, security skills, and organisational enablement. The current state is between the managed and defined levels, with a desired state of being quantitatively managed. The lack of training, communication, and employee satisfaction is a significant concern. Addressing these gaps requires a proactive approach encompassing situational awareness, a security-aware culture, and maximising user awareness. It is essential to focus on enabling staff with general and IIoT security skills and enhancing employee engagement with security staff at all levels. Additionally, providing tools to manage IIoT security, rewarding staff, and encouraging disclosure can significantly enhance employee satisfaction and productivity. By addressing these issues, organisations can improve the maturity of their security awareness and safeguard their IIoT devices, thereby creating a secure and trustworthy transport sector of SA.

A cybersecurity framework is developed and validated for IIoT in the SA transport sector to address the technological, organisational, procedural and people factors influencing IIoT cybersecurity in the SA transport sector. These mitigate the threats, vulnerabilities, and risks of IIoT cybersecurity in the transportation sector of South Africa. The cybersecurity framework is reviewed and validated against the MITRE ATT&CK framework for ICS. The addition of appropriate controls addressed the gaps identified.

References

Abdelaal, H. (2021, January 3). *Azure Defender for IoT Raw-Data and ICS MITRE ATT&CK Matrix Mapping via Azure Sentinel*, Microsoft Tech Community. Retrieved November 23, 2023, from https://techcommunity.microsoft.com/t5/microsoft-defender-for-iot-blog/azure-defender-for-iot-raw-data-and-ics-mitre-att-amp-ck-matrix/ba-p/1988171.

Abrams, M., & Weiss, J. (2008). *Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia*, Computer Security Resource Centre, National Institute of Standards and Technology, from http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

Acohido, B. (2015). *Improving Detection, Prevention and Response with Security Maturity Modeling*, SANS Institute InfoSec Reading Room, from https://www.sans.org/reading-room/whitepapers/analyst/improving-detection-prevention-response-security-maturity-modeling-35985.

Adaros Boye, C., Kearney, P., & Josephs, M. (2018). Cyber-risks in the industrial internet of things (IIoT): Towards a method for continuous assessment. In *Information Security: 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, Proceedings 21* (pp. 502-519). Springer International Publishing.

Adetoye, B., & Fong, R. C. W. (2023, January). Building a resilient cybersecurity workforce: A multidisciplinary solution to the problem of high turnover of cybersecurity analysts. In *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022* (pp. 61-87). Cham: Springer International Publishing.

AgileIT. (2023, January 3). *The Top 10 Biggest Cyberattacks of 2022*. AgileIT, Retrieved April 17, 2024, from https://www.agileit.com/news/biggest-cyberattacks-2022/.

Alfreds, D. (2016). *SA business 'unprepared' for cybercrime*, Fin24.com. Retrieved April 17, 2024, from http://www.fin24.com/Tech/Cyber-Security/sa-business-unprepared-for-cybercrime-20160609.

Akpan, F., Bendiab, G., Shiaeles, S., and Karamperidis, S. (2022). "Cybersecurity Challenges in the Maritime Sector. *Network*, 2, 123-138.

Allianz Global Corporate & Specialty. (2023). *Allianz Risk Barometer 2023*. Johannesburg/London/Munich/New York/Paris/São Paulo/Singapore: Allianz Global Corporate & Specialty. Creamer Media's Engineering News. Retrieved November 23, 2023, from

https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf.

Amoroso, E.G. (2013). *Cyber Attacks: Protecting National Infrastructure*, Student edition. Waltham, Butterworth-Heinemann., MA.

Andress, J., & Winterfield, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, Elsevier, MA.

Antrobus, R., Green, B., Frey, S., & Rashid, A. (2019). The forgotten I in IIoT: A vulnerability scanner for industrial Internet of Things.

Archon. (n.d.). *What are the Risks Associated with Industrial IoT (Industrial Internet of Things)?*, Archon. Retrieved November 23, 2023, from https://www.archonsecure.com/blog/what-are-the-risks-associated-with-industrial-iot.

Ashford, W. (2013). *Cyber attack shuts down Israeli toll road tunnel*, Computer Weekly. Retrieved 17 April 2024, from https://www.computerweekly.com/news/2240207924/Cyber-attack-shuts-down-Israeli-toll-road-tunnel.

Asomani-Boateng, R., Fricano, R. J., & Adarkwa, F. (2015). Assessing the socio-economic impacts of rural road improvements in Ghana: A case study of transport sector program support (II). *Case studies on transport policy*, *3*(4), 355-366.

Ayyagari, M. (2018). *Five Smart Ways How IoT is Transforming the Railways*, Cyient. Retrieved November 23, 2023, from https://www.cyient.com/blog/rail-transportation/five-smart-ways-how-iot-is-transforming-the-railways.

Bahaa, A., Abdelaziz, A., Sayed, A., Elfangary, L., & Fahmy, H. (2021). Monitoring real time security attacks for IoT systems using DevSecOps: a systematic literature review. *Information*, *12*(4), 154.

Baker, F. C. (2021). *Inadequacy of Existing Security Management Frameworks in Addressing Internet of Things (IoT) Cybersecurity-Related Risks* (Doctoral dissertation, Northcentral University).

Balaji, N. (2019, April 28). *GPS Tracking Apps Flaw Let Hackers Remotely Hijack the Car & Kill Engines to Create a Traffic Jam*. GBHackers. Retrieved November 23, 2023, from https://gbhackers.com/gps-tracking-apps/.

Bandara, O., Vidanagamachchi, K., & Wickramarachchi, R. (2019, March). A model for assessing maturity of industry 4.0 in the banking sector. In *Proceedings of the international conference on industrial engineering and operations management* (Vol. 2019).

Baran, G. (2019, March 28). *Shodan Monitor – New Tool to Setup Network Alerts and Track Devices Exposed to Internet*. GBHackers on Security. Retrieved November 23, 2023, from https://gbhackers.com/shodan-monitor-devices/.

Barrett. (2022, January). *Nexus Industrial Memory*. Retrieved March 22, 2024, from https://content.yudu.com/web/69r/0A4417d/EWorldDecJan22/html/index.html?refUrl=https%253A%252F%252Ff.xdref.com%252F&page=34.

Barrow, K. (2018). "Cybersecurity: guarding rail against evolving threats ", International Railway Journal, 15 April, [online], Retrieved December 7, 2023, from http://www.railjournal.com/index.php/technology/cybersecurity-guarding-rail-against-evolving-threats.html

Baruah, B., & Dhal, S. (2020, July). An efficient authentication scheme for secure communication between industrial IoT devices. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

BBC News. (2019, July 26). *Ransomware hits Johannesburg electricity supply*. BBC News. Retrieved November 23, 2023, from https://www.bbc.com/news/technology-49125853.

Bertin, C., & Mavoori, H. (2022). Innovative technology-based startup–large firm collaborations: influence of human and social capital on engagement and success. *IEEE Transactions on Engineering Management*.

Betts, D., & Richards. (2023, June 27). *Security best practices for IoT solutions*. Microsoft. Retrieved April 15, 2024, from https://learn.microsoft.com/en-us/azure/iot/iot-overview-security.

Bhaiyat, H., & Sithungu, S. (2022, June). The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure. In *European Conference on Cyber Warfare and Security* (Vol. 21, No. 1, pp. 46-51).

Bhattacharya, S. (2018). *The Top Ten IoT Vulnerabilities*, Infosec Institute. Retrieved November 23, 2023, from https://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/#gref

Biswas, A., & Wang, H. C. (2023, February 9). *Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain*. Sensors. Retrieved November 23, 2023, from https://doi.org/10.3390/s23041963.

Bitdefender. (2023). *THE 2023 IOT SECURITY LANDSCAPE REPORT*. Bitdefender. Retrieved 17 April 2024, from https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf.

Boehm, B. W. (1991). Software Risk Management: Principles and Practices, *IEEE Software* 8(1), 32-41.

Bolzonello, C. (2023, January 7). *Cyber defence must be a top priority for South African Business*. IOL. Retrieved November 23, 2023, from https://www.iol.co.za/business-report/companies/cyber-defence-must-be-a-top-priority-for-south-african-business-8eb0378b-7e61-44fb-8273-fa39da08b1d6.

Booth. (2021, July 28). *Transnet Cyberattack Could have Catastrophic Consequences*. Investec. Retrieved March 9, 2024, from https://www.investec.com/en_za/focus/economy/transnet-cyberattack-could-have-catastrophic-consequences.html.

Bowen, G. A. (2009). 'Document Analysis as a Qualitative Research Method', *Qualitative Research Journal* 9 (2), 27–40.

Bowne, M. (2015, August 18). *IOT vs. IIOT*. Retrieved from Profinet.com: http://us.profinet.com/iot-vs-IIoT/

Boye, C. A. (2021). *A Continuous Risk Management Approach for Cyber-Security in Industrial Control Systems* (Doctoral dissertation, Birmingham City University).

Brazier, A., Cooke, K., & Moravan, V. (2008). Using mixed methods for evaluating an integrative approach to cancer care: a case study. *Integrative Cancer Therapies*, *7*(1), 5-17.

Bronk, C. and Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. *Survival* 55(2), 81-96.

Brook, C. (2015). *Polish Planes Grounded After Airline Hit With DDoS Attack*, Threatpost. Retrieved April 17, 2024, from https://threatpost.com/polish-planes-grounded-after-airline-hit-with-ddos-attack/113412.

Burger, S. (2021, July 15). *IoT use in South Africa to grow by 14% a year to 2025*. Engineering News. Retrieved November 23, 2023, from https://www.engineeringnews.co.za/article/iot-use-in-south-africa-to-grow-by-14-a-year-to-2025-2021-07-15.

Burkhalter, M. (2022a). *IoT at sea -- how the internet of things powers the maritime industry*, Perle. Retrieved April 24, 2024, from https://www.perle.com/articles/iot-at-sea-how-the-internet-of-things-powers-the-maritime-industry-40193572.shtml.

Burkhalter. (2022b, January 24). *IoT and the Fourth Industrial Revolution*. Perle Systems. Retrieved April 10, 2024, from https://www.perle.com/articles/iot-and-the-fourth-industrial-revolution-40193554.shtml.

BusinessTech. (2022, March 18). *TransUnion cyber attack – hackers demand R225 million ransom*. BusinessTech. Retrieved November 23, 2023, from https://businesstech.co.za/news/cloud-hosting/569658/transunion-cyber-attack-hackers-demand-r225-million-ransom/.

Byres, E. (2012, September 5). *SCADA Security Basics: SCADA vs. ICS Terminology*. Tofino Security. Retrieved November 23, 2023, from https://www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology.

C&T RF Antennas Inc. (2021, November 17). *16 Wired and Wireless Communication Technologies in IoT*. C&T RF Antennas Inc. Retrieved November 23, 2023, from https://lcantennas.com/16-wired-and-wireless-communication-technologies-in-iot/.

Carroll, J. (2014). *Computer Security, 2nd ed*. Butterworths, USA.

Chan, B. (2017). *Industrial IoT versus IoT – do you know the difference?*, Strategy of things. Retrieved November 23, 2023, from https://strategyofthings.io/industrial-iot.

Chapman, J. (2022). *Cybersecurity Using ICS ATT&CK Strategies*. Global Cybersecurity Alliance. Retrieved November 23, 2023, from https://gca.isa.org/blog/cybersecurity-using-ics-attck-strategies.

Cheit, R. E. (1990). *Setting safety standards: Regulation in the public and private sectors*. Univ of California Press.

Chetty, P. (2022, October 19). *Correlation of variables in SPSS*. Knowledge Tank. Retrieved March 23, 2024, https://www.projectguru.in/correlation-variables-spss/

Chileshe, G., & van Heerden, R. (2012). SCADA Systems in South Africa and their Vulnerabilities. In V. L. (eds.) (Ed.), *Proceedings of the 7th International Conference of Information Warfare and Security* (pp. 90-97). UK: Academic Publishing Limited.

Cimpanu, C. (2017). University DDoSed by Its Own IoT Devices. *Bleeping Computer*. Retrieved November 23, 2023, from https://www.bleepingcomputer.com/news/security/university-ddosed-by-its-own-iot-devices/.

Cimpanu, C. (2018). *Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack*, Bleepingcomputer. Retrieved November 23, 2023, from https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack.

Cimpanu, C. (2019, June 25). *New Silex malware is bricking IoT devices, has scary plans*. ZDNet. Retrieved November 23, 2023, from https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/.

CIO Southeast Asia. (2022, November 29). *Shifts in threat landscape to industrial control systems in 2023: Research*. CIO Southeast Asia. Retrieved November 23, 2023, from https://ciosea.economictimes.indiatimes.com/news/security/shifts-in-threat-landscape-to-industrial-control-systems-in-2023-research/95832630.

Clayton, M. (2013). *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*, Christian Science Monitor. Retrieved November 23, 2023, from https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage.

CNBC Africa. (2017, January 26). *Transnet, GE have combined forces to bring the Industrial Internet to Africa*. CNBC Africa. Retrieved November 24, 2023, from https://www.cnbcafrica.com/news/2017/01/26/transnet-ge-combine-forces/.

Coldewey, D. (2019, January 30). *Cheap Internet of Things gadgets betray you even after you toss them in the trash*. Techcrunch. Retrieved November 24, 2023, from https://techcrunch.com/2019/01/30/cheap-internet-of-things-gadgets-betray-you-even-after-you-toss-them-in-the-trash/.

Collins, L. M. (2007, January 1). *Research Design and Methods*. Elsevier eBooks. https://doi.org/10.1016/b0-12-370870-2/00162-1

Constantin, L. (2019, May 22). *Over 90% of data transactions on IoT devices are unencrypted*. CSO. Retrieved November 24, 2023, from https://www.csoonline.com/article/567281/over-90-of-data-transactions-on-iot-devices-are-unencrypted.html.

CPNI. (2008). *Good practice guide Process Control and SCADA Security, Guide 1: Understand the business risk*, from http://www.cpni.gov.uk/Documents/Publications/2008/2008024-GPG_SCADA_Business_Risk.pdf.

Creswell, J. W. (2021). *A concise introduction to mixed methods research*. SAGE publications.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A. J., & Sheikh, A. (2011, June 27). *The case study approach*. BMC Medical Research Methodology (Online). Retrieved March 7, 2024, from https://doi.org/10.1186/1471-2288-11-100.

CyberPeace Institute. (n.d.). *Cyberattacks Impact and Harm on the Transportation sector | CyberPeace Institute*. cyberpeaceinstitute.org. Retrieved March 7, 2024, from https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/transportation.

Cybersecurity and Infrastructure Security Agency. (2020). Transportation Systems Sector. Retrieved March 24, 2024, from https://www.cisa.gov/transportation-systems-sector.

CyberKeel. (2014). Maritime cyber-risks: Virtual Pirates at Large on the Cyber Seas. Retrieved November 24, 2023, from http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf.

Dahbur, K., Mohammad, B. & Tarakji, A. B. (2011). 'A survey of risks, threats and vulnerabilities in cloud computing', *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications*, Amman, ACM, Jordan.

Darktrace. (2016). *Darktrace Discoveries: Global Threat Case Studies 2016*. Information Week. Retrieved November 24, 2023, from http://www.informationweek.com/whitepaper/cybersecurity/security/darktrace-discoveries-global-threat-case-studies-2016/383043.

DBSA. (n.d.). *How transportation is a key catalyst for economic growth in SA*. Development Bank of Southern Africa. Retrieved March 11, 2024, from https://www.dbsa.org/article/how-transportation-key-catalyst-economic-growth-sa.

Dhakal K. (2022). NVivo. *Journal of the Medical Library Association: JMLA*, *110*(2), 270–272. Retrieved March 11, 2024, from https://doi.org/10.5195/jmla.2022.1271.

Digital Directions Team. (2023, June 9). *IIOT vs IOT: Understanding Key Differences in Industrial and Consumer Applications*. Digital Directions. Retrieved November 24, 2023, from https://digitaldirections.com/IIoT-vs-iot-understanding-key-differences-in-industrial-and-consumer-applications/.

Directorate for Priority Crime Investigations. (2024). *Vision, Mission and Mandate*. SAPS. Retrieved April 24, 2024, from https://www.saps.gov.za/dpci/vision_mission_mandate.php.

Dovetail Editorial Team. (2023, February 27). *Validity in Research: A Guide to Better Results*. Retrieved February 28, 2024, from https://dovetail.com/research/validity-in-research/.

Dunn, J.E. (2013). *Hackers planted remote devices to smuggle drugs through Antwerp port*, Techworld.com. Retrieved November 24, 2023, from http://news.techworld.com/security/3474018/hackers-planted-remote-devices-to-smuggle-drugs-through-antwerp-port-europol-reveals/.

Edgar, T. W., & Manz, D. O. (2017). *Research Methods of Cyber Security*. Cambridge, MA: Syngress.

Empl, P., & Pernul, G. (2021, April). A flexible security analytics service for the industrial IoT. In *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems* (pp. 23-32).

ESRI. (2014). *The Geospatial Approach to Cybersecurity: An Executive Overview*. Esri. Retrieved November 24, 2023, from http://downloads.esri.com/support/whitepapers/other_/geospatial-approach-cybersecurity.pdf.

Farquharson, N., Mageto, J., & Makan, H. (2021). Effect of internet of things on road freight industry. *Journal of Transport and Supply Chain Management*. Retrieved November 24, 2023, from https://jtscm.co.za/index.php/jtscm/article/view/581.

Federal Bureau of Investigation. (2014). *2014 Internet Crime Report*, Internet Crime Compliant Centre. Retrieved November 24, 2023, from https://pdf.ic3.gov/2014_IC3Report.pdf.

Figueroa-Lorenzo, S., Añorga, J., & Arrizabalaga, S. (2020). A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS. *ACM Computing Surveys (CSUR)*, *53*(2), 1-53.

Fletcher, D., & Bye, P. (2022). *Cybersecurity in Transit Systems*. Washington, DC: The National Academies Press. Retrieved November 24, 2023, from https://nap.nationalacademies.org/catalog/26475/cybersecurity-in-transit-systems.

Fleury, N., Dubrunquez, T., & Alouani, I. (2021). Malware: An overview on threats, detection and evasion attacks. *arXiv preprint arXiv:2107.12873*.

Flick, U. (2009). An Introduction to Qualitative Research. 4thed. SAGE. pp. 32–36.

Forrest, C. (2016). *How the Mirai botnet almost took down an entire country, and what your business can learn*, Tech Republic. Retrieved November 25, 2023, from https://www.techrepublic.com/article/how-the-mirai-botnet-almost-took-down-an-entire-country-and-what-your-business-can-learn/.

Fortune Business Insights. (2023, April). *Internet of Things (IoT) Market*. Fortune Business Insights. Retrieved November 25, 2023, from https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307.

Fourie, P. (2020, January 19). *Should you buy an e-tag?* The North Coast Courier. Retrieved November 25, 2023, from https://northcoastcourier.co.za/147335/buy-e-tag/.

Fraser, L. (2023, May 13). *South Africa is facing a massive ransomware problem*. Businesstech. Retrieved November 25, 2023, from https://businesstech.co.za/news/technology/687131/south-africas-growing-ransomware-problem/.

Franklin, F. Jr. (2018). *7 Serious IoT Vulnerabilities*, DarkReading. Retrieved November 25, 2023, from https://www.darkreading.com/iot/7-serious-iot-vulnerabilities/d/d-id/1332616.

Fripp, C. (2016). *Anonymous hacks Armscor website with simple SQL injection,* htxt.*africa*. Retrieved November 25, 2023, from http://www.htxt.co.za/2016/07/12/armscor-website-hacked-sql-injection.

Gallagher, R., & Burkhardt, P. (2021, July 29). *'Death Kitty' Ransomware Linked to South African Port Attack*. Bloomberg. Retrieved November 25, 2023, from https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports#xj4y7vzkg.

Gartner. (2017, February 7). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. Gartner. Retrieved November 25, 2023, from http://www.gartner.com/newsroom/id/3598917.

Gebremichael, T., Ledwaba, L. P., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and privacy in the industrial internet of things: Current standards and future challenges. *IEEE Access*, *8*, 152351-152366.

Georgieva, E. (2022, September 19). *Uber's Internal Systems Compromised By An 18 Year Old*. Purplesec. Retrieved November 25, 2023, from https://purplesec.us/security-insights/uber-compromised-by-teenager.

Ghosh, S., Hughes, M., Hodgkinson, I., & Hughes, P. (2022). Digital transformation of industrial businesses: A dynamic capability approach. *Technovation*, *113*, 102414.

Goodin, D. (2023, May 2). *T-Mobile discloses 2nd data breach of 2023, this one leaking account PINs and more*. ARS Technica. Retrieved November 25, 2023, from https://arstechnica.com/information-technology/2023/05/t-mobile-discloses-2nd-data-breach-of-2023-this-one-leaking-account-pins-and-more.

Government of Republic of South Africa. (2002a). *Electronic Communications and Transactions Act*, Act 25 of 2002, Pretoria.

Government of Republic of South Africa. (2002b). *Regulation of Interception of Communications and Provision of Communication-Related Information Act*, Act 70 of 2002, Pretoria.

Government of Republic of South Africa. (2013). *Protection of Personal Information Act*, Act 4 of 2013, Pretoria.

Government of Republic of South Africa. (2020). *Cybercrimes Act*, Act 19 of 2020, Pretoria.

Government of UK. (2018). Code of Practice for Consumer IoT Security. Gov.uk. Retrieved November 25, 2023, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf.

Goward, D. (2019). GPS Jamming and Spoofing Reported at Port of Shanghai. *The Maritime Executive.* Retrieved November 25, 2023, from https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai.

Greenberg, A. (2015). *Hacker remotely kill a jeep on the highway - with me in it*, Wired. Retrieved 17 April 2024, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

Greig, J. (2023, June 13). *State-owned bank in South Africa confirms 'Akira' ransomware attack*. The Record. Retrieved November 25, 2023, https://therecord.media/development-bank-of-southern-africa-akira-ransomware-attack.

Grustniy, L. (2019, March 18). *Leonid Grustniy*. Kaspersky. Retrieved November 25, 2023, from https://www.kaspersky.com/blog/hacking-smart-car-alarm-systems/26014/.

Gunesh, R. (2016, July 20). *Research Methodology*. Rajgunesh. Retrieved November 25, 2023, from http://www.rajgunesh.com/resources/methodology.htm.

Hai-Jew. (n.d.). *Using NVivo: An Unofficial and Unauthorized Primer: Manual Coding in NVivo*. Scalar. Retrieved March 11, 2024, from https://scalar.usc.edu/works/using-nvivo-an-unofficial-and-unauthorized-primer/coding-in-nvivo.

Hasan, M. (2023, April 25). *15 Most Used IoT Protocols and Standards*. Ubuntu PIT. Retrieved November 25, 2023, from https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/.

Hassanzadeh, A., Modi, S., & Mulchandani, S. (2015, December). Towards effective security control assignment in the Industrial Internet of Things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 795-800). IEEE.

Hayes, A. (2023, October 31). *What Is a Confidence Interval and How Do You Calculate It?* Investopedia. Retrieved April 15, 2024, from https://www.investopedia.com/terms/c/confidenceinterval.asp.

Henning, C. (2015a, March 3). *IIoT is not IoT*. Profinet. Retrieved November 25, 2023, from http://us.profinet.com/IIoT-is-not-iot.

Henning, C. (2015b, September 1). *IOT and IIOT*. Profinet. Retrieved November 25, 2023, from http://us.profinet.com/iot-and-IIoT.

Henning, C. (2017, February 21). *7 Steps to IIOT*. Profinet. Retrieved November 25, 2023, from http://us.profinet.com/7-steps-IIoT.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105.

Higgins, K.J. (2015). *State Trooper Vehicles Hacked*, Dark Reading. Retrieved November 25, 2023, from http://www.darkreading.com/attacks-breaches/state-trooper-vehicles-hacked-/d/d-id/1322415.

Hindarto, D. (2023). Application Of Customer Service Enterprise Architecture In The Transportation Industry. *Journal of Computer Networks, Architecture and High Performance Computing*, *5*(2), 682-692.

Hirsch, S. (2019, April 3). *What are the challenges of managing cyber-attacks in a large company?* SocietyByte. Retrieved March 25, 2024, from https://www.societybyte.swiss/en/2019/04/03/what-are-the-challenges-of-managing-cyber-attacks-in-a-large-company/

Hitachi. (2017). *Daicel.com*. Hitachi and Daicel Develop Management and Manufacturing Dashboard by Utilizing IoT to Integrally Visualize KPIs from Management Information to Manufacturing Workplaces' Situations. Retrieved November 25, 2023, from https://www.daicel.com/data/news/00000576-1.pdf.

Hoffman, F. (2019). Industrial Internet of Things Vulnerabilities and Threats: What Stakeholder need to consider. *Issues in Information Systems*, *20*(1).

Hubeschle, A. (2011). *The Dark Side of the Internet: Cybercrime*. Institute of Security Studies Retrieved November 25, 2023, from http://www.issafrica.org/iss-today/the-dark-side-of-the-internet-cybercrime.

IIoT World. (2019, August 1). *Top risks to organizations in current IIoT environment*. IIoT World. Retrieved November 25, 2023, from https://www.IIoT-world.com/industrial-iot/connected-industry/top-risks-to-organizations-in-current-IIoT-environment.

Immuta. (n.d.). *What Is a Data Loss Prevention Policy?* Retrieved April 7, 2024, from https://www.immuta.com/guides/data-security-101/data-loss-prevention-policy.

Industrial Internet Consortium. (2016). Industrial Internet of Things Volume G4: Security Framework, Retrieved 15 April 2024, from https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf.

Institute of Directors in Southern Africa. 2009. The King Report on Corporate Governance for South Africa. Parklands, Cape Town: IDSA.

Irei, A., & Shea, S. (2024, January 30). *What is incident response? A complete guide*. Security. Retrieved March 26, 2024, from https://www.techtarget.com/searchsecurity/definition/incident-response.

ITIL. (2022). Information Technology Infrastructure Library (ITIL) version 4. PeopleCert.

IT News Africa. (2018, April 17). *Security a top trend for the future of IIoT*. IT News Africa. Retrieved November 25, 2023, from https://www.itnewsafrica.com/2018/04/security-a-top-trend-for-the-future-of-IIoT.

IT News Africa. (2022, November 16). *Ransomware Activity Doubles in Transportation and Shipping Industry*. IT News Africa. Retrieved November 25, 2023, from https://www.itnewsafrica.com/2022/11/ransomware-activity-doubles-in-transportation-and-shipping-industry.

ITU Publications. (2024). *Global Cybersecurity Index 2020*. Retrieved April 10, 2024, from https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

ITWeb. (2023, April 28). *South Africa ranked 5th on global cyber crime density list*. ITWeb. Retrieved November 25, 2023, from https://www.itweb.co.za/content/KA3WwMdz1nBvrydZ.

ISACA. (2010a). The Business Model for Information Security. USA.

ISACA. (2010b). ISACA Issues New Comprehensive Business Model for Information Security *In:* ISACA (ed.). USA: ISACA.

ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. Information Systems Audit and Control Association.

ISACA. (2023, May 19). ISACA 2022 Annual report. ISACA. Retrieved April 17, 2024, from https://heyzine.com/flip-book/c67626a563.html.

Ismail, S., Sitnikova, E., & Slay, J. (2015). SCADA systems cyber security for critical infrastructures: Case Studies in the Transport Sector. *Proceedings of the 10th International Conference on Cyber Warfare and Security* (ICCWS 2015), pp. 425-433.

ISO/IEC. (2022). *ISO 27002:2012 Code of practice for information security controls*, Pretoria: SABS Standards Division.

Ivezic, M. (2018). “Growing cyber-kinetic threats to railway systems”, CSO Online. Retrieved November 27, 2023, from https://www.csoonline.com/article/3281096/cyberwarfare/growing-cyber-kinetic-threats-to-railway-systems.html.

Jansen, J., & Van der Merwe, A. (2020). A Framework for Industrial Internet of Things. *Responsible Design, Implementation and Use of Information and Communication* (pp. 138-150). Skukuza: Springer.

Jayalaxmi, P., Saha, R., Kumar, G., Kumar, N., & Kim, T. H. (2021). A taxonomy of security issues in Industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges. *IEEE Access*, *9*, 25344-25359.

Johnson, A. (2023, January 31). *Security, IoT and Red Flags Starting Off 2023*. Gartner. Retrieved November 27, 2023, https://blogs.gartner.com/andrew-johnson/security-iot-and-red-flags-starting-off-2023.

Johnson, J. (2017, June 15). “Securing Industrial IoT: There is no simple answer”. *IIoT World*. Retrieved November 27, 2023, from https://www.IIoT-world.com/ics-security/cybersecurity/securing-industrial-iot-there-are-no-simple-solutions.

Jones, A. (2013). *Information Security Incident Management Procedures*, Heriot-Watt University. Retrieved November 27, 2023, from https://www.hw.ac.uk/documents/information-security-incident-management-procedures.pdf.

Kan, M. (2016). DDoS attack on Dyn came from 100,000 infected devices. *Computer World*. Retrieved November 27, 2023, from http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html.

Kapkaeva, N., Gurzhiy, A., Maydanova, S., and Levina, A. (2021). “Digital Platform for Maritime Port Ecosystem: Port of Hamburg Case”. *Transportation Research Procedia*, 54, 909-917.

Kerner, S. M. (2022, April 26). *Colonial Pipeline hack explained: Everything you need to know*. WhatIs. Viewed 17 April 2024, from https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Khanduri, A. (2022). *People, Process, Technology: The PPT Framework, Explained*. Plutora. Retrieved November 27, 2023, from https://www.plutora.com/blog/people-process-technology-ppt-framework-explained.

Kianpour, M., & Raza, S. (2024). More than malware: unmasking the hidden risk of cybersecurity regulations. *International Cybersecurity Law Review*, 1-44.

Kirk, J. (2009). *Virus Attacks Ministry of Defence*, CIO.co.uk. Retrieved November 27, 2023, from http://www.cio.co.uk/news/3460/virus-attacks-ministry-of-defence/.

Knox, J. (2015, June 15). Coast Guard Commandant on Cyber in the maritime domain, US Coast Guard. Retrieved November 27, 2023, from https://mariners.coastguard.blog/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/.

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. *IEEE Access*, *8*, 209802-209834.

Kour, R., Karim, R., & Thaduri, A. (2020). Cybersecurity for railways–A maturity model. *Proceedings of the institution of mechanical engineers, Part F: Journal of Rail and Rapid Transit*, *234*(10), 1129-1148.

Kovacs, E. (2014). Default password exposes digital highway signs to hacker attacks. *Security Week.* Retrieved November 27, 2023, from http://www.securityweek.com/default-password-exposes-digital-highway-signs-hacker-attacks.

Kravets, D. (2009). Feds: hacker disabled offshore oil platforms' leak detection system. *Wired*, 18 March, viewed 27 November 2023 from https://www.wired.com/2009/03/feds-hacker-dis/.

Krebs, B. (2014). *Target Hackers Broke in via HVAC Company*, Krebs on Security Blog. Retrieved November 27, 2023, from http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

Krutz, R.L. (2006). *Securing SCADA Systems*, Wiley, Indianapolis.

Ku, R., and Weiss, J. (2017). *Integrating Security into the IoT Strategy in the New Converged Environment*. Trend Micro Incorporated.

Kuechler W, Vaishnavi V (2012). A framework for theory development in design science research: Multiple perspectives. *Journal of the Association for Information Systems* 13(6): 395–423.

Kumar, R., Sindhwani, R., & Singh, P. L. (2022). IIoT implementation challenges: Analysis and mitigation by blockchain. *Journal of Global Operations and Strategic Sourcing*, *15*(3), 363-379.

Kumar, S., Tiwari, P., & Zymbler, M. (2019, December 1). *Internet of Things is a revolutionary approach for future technology enhancement: a review*. Journal of Big Data. https://doi.org/10.1186/s40537-019-0268-2

KVH Watch. (2021). “How Using Dedicated Maritime IoT Connectivity Produces Cost Savings”. Maritime Executive. Retrieved November 27, 2023, from https://www.maritime-executive.com/features/how-using-dedicated-maritime-iot-connectivity-produces-cost-savings.

Laszka, A., Abbas, W., Vorobeychik, Y., & Koutsoukos, X. (2020). Integrating redundancy, diversity, and hardening to improve security of industrial internet of things. *Cyber-Physical Systems*, *6*(1), 1-32.

Latesthackingnews (2017, January 11). *Hackers Can Stop Pacemakers and Kill Patients Warns US Government*, Latest Hacking News. Retrieved November 27, 2023, from https://latesthackingnews.com/2017/01/11/hackers-can-stop-pacemakers-and-kill-patients-warns-us-government.

Leyden, J. (2008). *Polish teen derails tram after hacking train network*, The Register. Retrieved November 27, 2023, from http://www.theregister.co.uk/2008/01/11/tram_hack.

Lightfoot, L. (2023, March 28). *The Top 10 Biggest Cyber Attacks Of 2021*. Expertinsights.com. Retrieved November 27, 2023, from https://expertinsights.com/insights/10-high-profile-attacks-2021.

Lomas, N. (2015, February 10). Samsung Edits Orwellian Clause Out of TV Privacy Policy. *Tech Crunch*. Retrieved November 27, 2023, from https://techcrunch.com/2015/02/10/smarttv-privacy/.

Madakam, S., & Uchiya, T. (2019). Industrial internet of things (IIoT): principles, processes and protocols. *The Internet of Things in the Industrial Sector: Security and Device Connectivity, Smart Environments, and Industry 4.0*, 35-53.

Maliti, S. (2023, February 16). *Postbank suffered yet another ‘malicious’ cyber incident in December*. IOL. Retrieved November 27, 2023, from https://www.iol.co.za/capeargus/news/postbank-suffered-yet-another-malicious-cyber-incident-in-december-8dcd6d77-f988-4aeb-92b6-ccc437c9c720.

Malware News. (2020, April). *Telling-the-full-story-with-the-mitre-att-ck-for-ics-framework*, Malware News. Retrieved November 27, 2023, from https://malware.news/t/telling-the-full-story-with-the-mitre-att-ck-for-ics-framework/38884.

Mamiit, A. (2019, June 22). *NASA hacked: 500 MB of mission data stolen through a Raspberry Pi computer*. Digitaltrends. Retrieved November 27, 2023, from https://www.digitaltrends.com/computing/hackers-steal-500-mb-nasa-data-raspberry-pi.

Manditereza, K. (2017, June 8). *4 Key Differences Between SCADA and Industrial IoT*. LinkedIn. Retrieved November 27, 2023, from https://www.linkedin.com/pulse/4-key-differences-between-scada-industrial-iot-kudzai-manditereza.

March, S.T. & Smith, G. (1995). Design and natural science research on information technology. *Decision Support Systems* 15(4): 251–266

March, S. T. & Storey, V. C. (2008). Design science in the information systems discipline: an introduction to the special issue on design science research. Management Information Systems Quarterly, 32(4), 6.

MathBits. (2016). *Correlation Coefficient*, MathBits.com. Retrieved November 27, 2023, from http://mathbits.com/MathBits/TISection/Statistics2/correlation.htm.

Matsumoto, N., Fujita, J., Endoh, H., Yamada, T., Sawada, K., & Kaneko, O. (2021). Asset management method of industrial IoT systems for cyber-security countermeasures. *Information*, *12*(11), 460.

Manditereza, K. (2017, June 8). *4 Key Differences Between SCADA and Industrial IoT*, LinkedIn. Retrieved November 27, 2023, from https://www.linkedin.com/pulse/4-key-differences-between-scada-industrial-iot-kudzai-manditereza.

Martin, D. (2022, October 11). *7 IoT and OT Cyber Risks in the Transportation Industry*. GlobalTrade. Retrieved November 27, 2023, https://www.globaltrademag.com/7-iot-and-ot-cyber-risks-in-the-transportation-industry.

Matlhabe, G. (2022, October 24). *SA has highest number of targeted ransomware, business email cyber attacks in Africa*. IOL. Retrieved November 27, 2023, from https://www.iol.co.za/pretoria-news/news/sa-has-highest-number-of-targeted-ransomware-business-email-cyber-attacks-in-africa-382d45a8-6b9a-41a0-8e5d-a3e0d0402676.

Maxime, A., Tibirna, & TDR. (2024, January 4). *The Transportation sector cyber threat overview*. IO Sekoia Blog. Retrieved March 22, 2024, from https://blog.sekoia.io/the-transportation-sector-cyber-threat-overview.

McCallister, E. (2010). *Guide to protecting the confidentiality of personally identifiable information*. Diane Publishing.

McCue, A. (2003). *'Revenge' hack downed US port systems*. ZDNet. Retrieved November 27, 2023, from http://www.zdnet.com/article/revenge-hack-downed-us-port-systems.

McKee, M. (2019, April 25). *Insider Threats: Manufacturing's Silent Scourge*. Industry Week. Retrieved November 27, 2023, from https://www.industryweek.com/technology-and-IIoT/article/22027503/insider-threats-manufacturings-silent-scourge.

Microsoft. (n.d.). *What Is Access Control?* Microsoft.com. Retrieved April 7, 2024, from https://www.microsoft.com/en-za/security/business/security-101/what-is-access-control.

Miller, A. (2021, October 19). *Cybersecurity Attacks & the Transportation Industry*. Cyber Management Alliance. Retrieved November 27, 2023, https://www.cm-alliance.com/cybersecurity-blog/cybersecurity-attacks-the-transportation-industry.

Miller, B., & Rowe, D. (2012). A Survey of SCADA and Critical Infrastructure Incidents. *Proceedings of the 1st Annual conference on Research in information technology* (pp. 51-56). New York: ACM.

Min, H. (2022). "Developing a smart port architecture and essential elements in the era of Industry 4.0". *Maritime Economics & Logistics*, pp. 24, 189–207.

Minett, A. (2022, April 26). *How Often Should Risk Assessments Be Carried Out, and When Should Risk Controls Be Reviewed?* CHAS. Retrieved April 4, 2024, from https://www.chas.co.uk/blog/how-often-risk-assessments-reviewed.

Mkhwananzi, S. (2015). *Roads agency account hacked for R8.5m*, iol.co.za. Retrieved November 27, 2023, from http://www.iol.co.za/capetimes/roads-agency-account-hacked-for-r8-5m-1.1928834.

Mngadi, W. B., & Justice, C. (2021). *An analysis of cybercrime investigatation by Directorate for priority crim investigation*. [Master's thesis, University of South Africa]. https://uir.unisa.ac.za/handle/10500/28659?show=full

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

Molavi, A., Lim, G., and Race, B. (2019). "A Framework for Building a Smart Port and Smart Port Index". *International Journal of Sustainable Transportation*, 14(9), 686-700.

Mouratidis, H., & Diamantopoulou, V. (2018). A security analysis method for industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*(9), 4093-4100.

Moyo, A. (2020, February 05). *Tracker hack hints at more ransomware attacks in SA*. ITWeb. Retrieved November 27, 2023, from https://www.itweb.co.za/content/LPp6VMr4YxNvDKQz.

Moyo, A. (2022, June 17). *RansomHouse hackers threaten to sell Shoprite data*. Retrieved November 13, 2024, from ITWeb: https://www.itweb.co.za/content/JBwEr7n3NZEM6Db2.

Moyo, A. (2023, July 6). *More POPIA fines on the horizon, warns InfoReg*. ITWeb. Retrieved March 22, 2024, from https://www.itweb.co.za/article/more-popia-fines-on-the-horizon-warns-inforeg/8OKdWMDXrVLMbznQ

Mphahlele, T. (2016, 18 October). *Port of Durban gets smart technology*. Retrieved 16 November 2023, from BiznisAfrica: https://www.biznisafrica.com/port-of-durban-gets-smart-technology/

MSC. (n.d.). *Smart containers*. Retrieved November 16, 2023, from MSC: https://www.msc.com/en/solutions/digital-solutions/smart-containers

Muhammad, I. J., & Iqbal, M. M. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). *International Conference on Communication Technologies (ComTech)* (pp. 78-90). Rawalpindi, Pakistan: IEEE.

Mybroadband. (2017, September 28). *SqwidNet IoT network in South Africa growing fast*. Mybroadband.co.za. Retrieved April 20, 2024, from: https://mybroadband.co.za/news/cellular/230823-sqwidnet-iot-network-in-south-africa-growing-fast.html.

Nagaraj, V. (2014, February 26). *The Industrial IoT Isn't the Same as the Consumer IoT*, Forbes. Retrieved November 27, 2023, from https://www.forbes.com/sites/oreillymedia/2014/02/26/the-industrial-iot-isnt-the-same-as-the-consumer-iot/#6685c5864720

Nakashima, E. & Warrick, J. (2012). *Stuxnet was the work of U.S. and Israel, officials say*, Washington Post. Retrieved November 27, 2023, from http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Nakashima, E., Miller, G. & Tate, J. (2012). *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*, Washington Post. Retrieved November 27, 2023, from http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

Ndaliso, C. (2018, 23 January). *Transnet loses smartphone load to thieves*. iol.co.za. Retrieved November 27, 2023, from https://www.iol.co.za/dailynews/transnet-loses-smartphone-load-to-thieves-12870525.

Ndlovu, M. (2023, May 19). *Spyware attacks in South Africa increase by 18.8%*. Mail&Guardian. Retrieved November 28, 2023, from https://mg.co.za/article/2023-05-19-spyware-attacks-in-south-africa-increase-by-18-8.

Ngwenya, M., & Ngoepe, M. (2020). A framework for data security, privacy, and trust in "consumer internet of things" assemblages in South Africa. *DOI:10.1002/spy2.122*, 1-10.

National Institute of Standards and Technology (NIST). (2019). NISTIR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks.

Nvivo. (2021). *Nvivo 12 Help*. Retrieved August 12, 2024, from https://help-nv.qsrinternational.com/12/win/v12.1.115-d3ea61/Content/nodes/review-references-in-a-node.htm

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009, May). Outline of a design science research process. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology* (pp. 1-11).

Okeke, F. (2022, November 23). *Top 6 security risks associated with industrial IoT*. TechRepublic. Retrieved November 28, 2023, from https://www.techrepublic.com/article/top-security-risks-industrial-iot.

Oladimeji, D., Gupta, K., Kose, N. A., Gundogan, K., Ge, L., & Liang. (2023, April 11). *Smart Transportation: An Overview of Technologies and Applications*. Sensors. https://doi.org/10.3390/s23083880

Opperman, I. (2023, November 28). *Chaos at ports will cost the country, businesses and consumers*. The Citizen. Retrieved April 12, 2024, from https://www.citizen.co.za/business/chaos-at-ports-will-cost-country-businesses-and-consumers.

OWASP (n.d.) "IoT Vulnerabilities Project", OWASP. Retrieved November 28, 2023, from https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#IoT_Vulnerabilities

Pagliara, F., Aria, M., Russo, L., & Della Corte, V. (2021). A theoretical model linking the development of the transportation system with citizens' trust in government actors. *Papers in Regional Science, 100*(1), 273-286.

Paloika, & Klubnikin. (2023, August 19). *Top 5 Industrial IoT (IIoT) security challenges & ways to overcome them*. ITRex. Retrieved April 12, 2024, from https://itrexgroup.com/blog/iiot-security-challenges.

Patrick, H. (2016). 'Security information flow in the public sector: KZN Health and Education', PhD Thesis, School of Management, Information and Governance, University of KwaZulu-Natal.

Patton, M.L. (2005). *Understanding research methods*, Pyrczak, Glendale, California.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V. & Bragge, J. (2006). The design science research process: a model for producing and presenting information systems research.

Penta Security. (2023, August 14). *The Rise of Cyberattacks on the Transport Sector: What Are the Risks?* Penta Security Inc. Retrieved March 7, 2024, from https://www.pentasecurity.com/blog/cyberattacks-transport-sector-what-risks.

Peterson, T. (2018, 3 August). Cape Town's burning trains: Here's what could be behind the destruction. News24.co.za. Retrieved November 28, 2023, from https://www.news24.com/SouthAfrica/News/cape-towns-burning-trains-heres-what-could-be-behind-the-destruction-20180803.

Pohl, F., & Schotten, H. D. (2017). Secure and scalable remote access tunnels for the IIoT: An assessment of openVPN and IPsec performance. In *Service-Oriented and Cloud Computing: 6th IFIP WG 2.14 European Conference, ESOCC 2017, Oslo, Norway, September 27-29, 2017, Proceedings 6* (pp. 83-90). Springer International Publishing.

Postscapes. (2020, February 1). *IoT Standards and Protocols,* Postscapes. Retrieved November 28, 2023, from https://www.postscapes.com/internet-of-things-protocols.

Pretorius, B. (2016). Cyber-Security and Governance for Industrial Control Systems (ICS) in South Africa. South Africa: University of Kwazulu-Natal.

Pretorius, B., & Van Niekerk, B. (2019). IIoT Security: Do I really need a Firewall for my Train? *The Proceeding of the 14th International Conference on Cyber Warfare and Security* (pp. 338-347). UK: Academic Conferences and Publishing International Limited.

Pretorius, B., & Van Niekerk, B. (2020). Industrial Internet of Things Security for the Transportation Infrastructure. *Journal of Information Warfare, 19*(3), 50-67. Retrieved from https://www.jstor.org/stable/27033632.

Pretorius, B., & Van Niekerk, B. (2023). IOT and IIOT Security for the South African Maritime and Freight Transport Sectors. *Scientia Militaria: South African Journal of Military Studies*, *51*(3), 133-160.

Project SHINE., (2014). *Project SHINE (SHodan INtelligence Extraction) Findings Report*, scadahacker.com. Retrieved November 28, 2023, from https://scadahacker.com/library/Documents/ICS_Vulnerabilities/Infracritical%20-%20Project%20SHINE%20Findings%20Report%20-%20Oct%202014.pdf.

QC Staff. (2023, September 3). *What are the Cyber Threats and Risk Factors in Transportation*. Quality Carriers. Retrieved March 22, 2024, from https://qualitycarriers.com/company-news/understanding-cyber-security-threats-and-risk-factors-in-the-transportation-sector.

Qi, S., Lu, Y., Wei, W., & Chen, X. (2020). Efficient data access control with fine-grained data protection in cloud-assisted IIoT. *IEEE Internet of Things Journal*, *8*(4), 2886-2899.

Ragan, S. (2012, January 25). *Railway Network Disrupted after Cyber Attack, Report Says*. Security Week. Retrieved November 29, 2023, from http://www.securityweek.com/railway-network-disruptedafter-cyber-attack-report-says.

Rajiv. (2022, July 31). *What are the major components of Internet of Things*. RF Page. Retrieved November 29, 2023, from https://www.rfpage.com/what-are-the-major-components-of-internet-of-things.

Rasool, F. (2012). *KPMG investigates Postbank theft*, ITWeb Security. Retrieved November 29, 2023, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=50919:kpmg-investigates-postbank-theft&catid=234.

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *Sage Open*, 11(1). https://doi.org/10.1177/21582440211000049

Rhodes-Ousley, M. (2013). *The Complete Reference: Information Security 2nd edition*, The McGraw-Hill Companies.

Rodionov, E. (2012). *Interconnection of Gauss with Stuxnet, Duqu & Flame*, ESET Blog. Retrieved November 29, 2023, from http://blog.eset.com/2012/08/15/interconnection-of-gauss-with-stuxnet-duqu-flame.

Rodriguez, E., & Edwards, J. (2010). People, technology, processes and risk knowledge sharing. *Proceedings of the European Conference on Knowledge Management.* ECKM.

RSA. (2014). *RSA Security Awareness Program*, EMC. Retrieved November 29, 2023, from http://www.emc.com/collateral/data-sheet/h13289-ds-rsa-security-awareness-program.pdf.

Rubin, A. (2008). *Practioner's guide to using research for evidence-based practice*, John Wiley, Hoboken, New Jersey.

Sakovich, N. (2023, May 12). *Internet of Things (IoT) Protocols and Connectivity Options: An Overview*. Sam Solutions. Retrieved November 29, 2023, from https://www.sam-solutions.com/blog/internet-of-things-iot-protocols-and-connectivity-options-an-overview.

Sammon, J. P., & Caverly, R. J. (2007). Transportation systems: critical infrastructure and key resources sector-specific plan as input to the National Infrastructure Protection Plan. *Homeland Security Dept.*

SANS Institute. (2006). *An Introduction to Information System Risk Management*, Retrieved November 29, 2023, from https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204.

SANS Institute. (2012). *Insider Threat Risk Formula: Survivability, Risk and threat*. SANS. Retrieved November 29, 2023, from https://cyber-defense.sans.org/blog/2012/10/23/insider-threat-risk-formula-survivability-risk-and-threat.

SANS Institute. (2016). *CIS Critical Security Controls*, SANS. Retrieved April 20, 2024, from https://www.sans.org/critical-security-controls.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research Methods for Business Students. Pearson Education.

Saunders, M. N., Lewis, P., Thornhill, A., & Bristow, A. (2015). Understanding research philosophy and approaches to theory development.

Saunders, M., & Tosey, P. (2013). *The Layers of Research Design*. Academia. Retrieved November 29, 2023, from https://www.academia.edu/4107831/The_Layers_of_Research_Design.

Schiffer, A. (2017, July 21). *How a fish tank helped hack a casino*. The Washington Post. Retrieved November 29, 2023, from https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/.

Seacom. (2022, July 28). *8 out of 10 enterprises have been targeted in cyber attacks*. Seacom. Retrieved November 29, 2023, from https://seacom.co.za/business-insights/8-out-of-10-enterprises-have-been-targeted-in-cyber-attacks/.

Seacom. (2023, January 20). *SA has highest number of ransomware and email attacks in Africa*. Seacom. Retrieved November 29, 2023, from https://seacom.co.za/business-insights/sa-has-highest-number-of-ransomware-and-email-attacks-in-africa/.

Security of Critical Infrastructure Act 2018. (2018). No. 29 of 2018, Australian Government. Retrieved November 29, 2023, from https://www.legislation.gov.au/Details/C2018A00029/Download.

Security Magazine. (2020, October 20). *Maritime Industry Sees 400% Increase in Attempted Cyberattacks Since February 2020*. Retrieved March 9, 2024, from

https://www.securitymagazine.com/articles/92541-maritime-industry-sees-400-increase-in-attempted-cyberattacks-since-february-2020.

Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, *149*, 102481.

Sha, L., Xiao, F., Chen, W., & Sun, J. (2018). IIoT-SIDefender: Detecting and defense against the sensitive information leakage in industry IoT. *World Wide Web*, *21*, 59-88.

Shah, S. H. H., Madni, S. H. H., Hashim, S., Ali, J., & Faheem, M. (2024, January 16). *Factors influencing the adoption of industrial internet of things for the manufacturing and production small and medium enterprises in developing countries.* IET Collaborative Intelligent Manufacturing. https://doi.org/10.1049/cim2.12093

Shahriar, H. & Zulkernine, M. (2012). 'Mitigating program security vulnerabilities: Approaches and challenges', *ACM* 44**,** 1-46. Retrieved November 29, 2023, from http://dl.acm.org/citation.cfm?id=2187673.

Shilenge, M., & Telukdarie, A. (2021). 4IR integration of information technology best practice framework in operational technology. *Journal of Industrial Engineering and Management (JIEM)*, *14*(3), 457-476.

Smith, C. (2021, July 30). *Transnet cyberattack: Main ports at 100%, but warehousing and cold storage still impacted*. News24. Retrieved January 24, 2024, from https://www.news24.com/fin24/economy/transnet-cyberattack-main-ports-at-100-but-warehousing-and-cold-storage-still-impacted-20210730.

SOCRadar. (2022, October 19). *Sensitive Data of 65,000+ Entities in 111 Countries Leaked due to a Single Misconfigured Data Bucket*. SOCRadar. Retrieved November 29, 2023, from https://socradar.io/sensitive-data-of-65000-entities-in-111-countries-leaked-due-to-a-single-misconfigured-data-bucket.

Solomon, H. (2022, June). *Many OT products are 'insecure by design,' say researchers*. IT World Canada, 22 June. Retrieved November 29, 2023, from https://www.itworldcanada.com/article/many-ot-products-are-insecure-by-design-say-researchers/489735.

Solomon, M. (2016). *Anonymous Africa cyber hackers shut down Gupta-linked websites*, Mail and Guardian. Retrieved November 29, 2023, from http://mg.co.za/article/2016-06-15-anonymous-africa-cyber-hackers-shutdown-gupta-linked-websites.

Starr, M. (2014, January 19). *Fridge caught sending spam emails in botnet attack*. CNET. Retrieved November 29, 2023, from http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/.

Stouffer, K., Falco, J., Kent, K. (2006). *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, National Institute of Standards and Technology Special Publication 800-82.

Subramanian, A. (2023, November 4) *Strategic GRC Implementation Roadmap with Timeline for Modern Business*. LinkedIn. Retrieved April 7, 2024, from https://www.linkedin.com/posts/raydalio_changingworldorder-booklaunch-activity-6875877869655080960-nw6W.

Sullivan, P. (2020). *Critical IIoT security risks cloud IoT's expansion into industry*. Tech Target. Retrieved November 29, 2023, from https://www.techtarget.com/searchsecurity/tip/Critical-IIoT-security-risks-cloud-IoTs-expansion-into-industry.

Susanto, H., Almunawar, M. N. & Tuan, Y. C. (2012). 'Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level', *International Journal of Engineering and Technology* 2, 67-75.

Swanbeck, S. (2015, June 22). *Coast Guard Commandant Addresses Cybersecurity Vulnerabilities on Offshore Oil Rigs*, Center for Strategic and International Studies. Retrieved November 29, 2023, from https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities.

Symantec. (2018). "Internet Security Threat Report, Volume 23", April, Symantec. Retrieved November 29, 2023, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

Symantec Threat Hunter Team. (2023, May 15). *Lancefly: Group Uses Custom Backdoor to Target Orgs in Government, Aviation, Other Sectors*, Symantec Enterprise Blogs. Retrieved March 22, 2024, from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor.

Szuba, T. (1998). Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security. United States: National Center for Education Statistics.

Taber, K. S. (2017, June 7). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. Research in Science Education. https://doi.org/10.1007/s11165-016-9602-2.

Talabis, M. M., McPherson, R., Miyamoto, I., & Martin, J. L. (2015). Information Security Analytics - Finding Security Insights, Patterns, and Anomalies in Big Data. Waltham, MA: Syngress.

Teddlie, C., & Tashakkori, A. (2006). A general typology of research designs featuring mixed methods. *Research in the Schools*, *13*(1), 12-28.

iONLINE. (2023, November 28). *IoT boom expected in South Africa*. TechCentral. Retrieved April 22, 2024, from https://techcentral.co.za/iot-boom-south-africa-ionline-ionpr/236005/.

Temizel, A., Halici, T., Logoglu, B., Temizel, T. T., Omruuzun, F., & Karaman, E. (2011). Experiences on image and video processing with CUDA and OpenCL. In *GPU computing gems Emerald Edition* (pp. 547-567). Morgan Kaufmann.

Tezer, O. S. (2013, December 23). *An Advanced Message Queuing Protocol (AMQP) Walkthrough*, DigitalOcean. Retrieved November 29, 2023, from https://www.digitalocean.com/community/tutorials/an-advanced-message-queuing-protocol-amqp-walkthrough.

The Guardian. (2024, March 14). *Russia suspected of jamming GPS signal on aircraft carrying Grant Shapps*. Retrieved April 12, 2024, from https://www.theguardian.com/politics/2024/mar/14/russia-suspected-of-jamming-gps-signal-on-aircraft-carrying-grant-shapps.

The MITRE Corporation. (2020a, May 21). *I/O Image, Technique T0877 - ICS*. MITRE ATT&CK. Retrieved April 25, 2024, from https://attack.mitre.org/techniques/T0877/.

The MITRE Corporation. (2020b, May 21). *Monitor Process State, Technique T0801 - ICS*. MITRE ATT&CK. Retrieved April 25, 2024, from https://attack.mitre.org/techniques/T0801/.

The MITRE Corporation. (2020c, May 21). *Screen Capture, Technique T0852 - ICS*. MITRE ATT&CK. Retrieved April 25, 2024, from https://attack.mitre.org/techniques/T0852/.

The MITRE Corporation. (2020d, May 21). *Manipulate I/O Image, Technique T0835 - ICS*. MITRE ATT&CK. Retrieved April 25, 2024, from https://attack.mitre.org/techniques/T0835/.

The MITRE Corporation. (2023a, October 13). *Supply Chain Compromise, Technique T0862* - ICS. MITRE ATT&CK. Retrieved April 7, 2024, from https://attack.mitre.org/techniques/T0862/.

The MITRE Corporation. (2023b, March 30). *Data Loss Prevention, Mitigation M0803 - ICS,* MITRE ATT&CK. Retrieved April 7, 2024, from https://attack.mitre.org/mitigations/M0803/.

The MITRE Corporation. (2023c). MITRE ATT&CK. Retrieved April 7, 2024, from MITRE ATT&CK: https://attack.mitre.org/

Theoharidou, M., Kandias, M., Gritzalis, D. (2012). Securing Transportation-Critical Infrastructures: Trends and Perspectives. In: Georgiadis, C.K., Jahankhani, H., Pimenidis, E., Bashroush, R., Al-Nemrat, A. (eds) *Global Security, Safety and Sustainability & e-Democracy. e-Democracy* ICGS3 2011 2011. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol 99. Springer, Berlin, Heidelberg.

TimesLIVE. (2021, July 29). *Food crisis loading? Products at risk of going off and animal feed stuck at Durban port*, TimesLIVE. Retrieved April 24, 2024, from https://www.timeslive.co.za/news/south-africa/2021-07-29-food-crisis-loading-products-at-risk-of-going-off-and-animal-feed-stuck-at-durban-port/.

Tunny. (n.d.). *Do you need a policy on policies?,* Effective Governance. Retrieved April 3, 2024, from https://www.effectivegovernance.com.au/page/knowledge-centre/news-articles/do-you-need-a-policy-on-policies.

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

U.S. Department of Homeland Security. (2015, June 26). *Transportation Systems Sector Cybersecurity Framework Implementation Guidance*, CISA.gov. Retrieved April 16, 2024, from https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf.

Vada, H. A. L. V. O. R. (2022). Comparative analysis of multi-factor authentication schemes for Internet of Things (bachelor's thesis, University of Twente).

Van Zyl, G. (2016). *Anonymous' hacks' Armscor website*, Fin24.com, Retrieved November 29, 2023, from http://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712.

Van Niekerk, B. (2017). Analysis of cyber-attacks against the transportation sector. In: M.E. Korstanje (ed.), *Threat mitigation and detection of cyber warfare and terrorism activities*, ed., Hershey, PA: IGI-Global, pp. 68-91.

Valderrama, M. E., Monroy, Á. I. C., & Behrentz, E. (2019). Challenges in greenhouse gas mitigation in developing countries: A case study of the Colombian transport sector. *Energy policy*, *124*, 111-122.

Vaughan-Nichols, S. (2019, December 3). *FBI warns about snoopy smart TVs spying on you*, ZDNet. Retrieved November 29, 2023, from https://www.zdnet.com/article/fbi-warns-about-snoopy-smart-tvs-spying-on-you/.

Venktess, K. (2017, March 12). *SA Internet of Things firm set for global expansion on R100m boost*. Fin24.com, Retrieved November 29, 2023, from http://www.fin24.com/Tech/News/sa-iot-company-to-expand-globally-after-r100m-boost-20170310.

Verizon. (2023). Verizon 2023 Data Breach Investigations Report. New York: Verizon. Retrieved November 29, 2023, from https://www.verizon.com/business/resources/Tff/reports/2023-data-breach-investigations-report-dbir.pdf.

Vermeulen, J. (2016a). *Anonymous hacks SA government database*, Mybroadband.co.za. Retrieved November 29, 2023, from http://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html.

Vermeulen, J. (2016b). *This is how I took down the SABC: Anonymous hacker*, Mybroadband.co.za. Retrieved November 29, 2023, from http://mybroadband.co.za/news/security/168303-this-is-how-i-took-down-the-sabc-anonymous-hacker.html.

Wagstaff, J. (2014). *All at sea: global shipping fleet exposed to hacking threat*, Reuters. Retrieved November 29, 2023, from http://www.reuters.com/article/2014/04/24/tech-cybersecurity-shipping-graphic-pix-idUSL3N0NG0GP20140424.

Waldman, A. (2022). *Tenable: 72% of organizations remain vulnerable to Log4Shell*, TechTarget. Retrieved November 29, 2023, from https://www.techtarget.com/searchsecurity/news/252527814/Tenable-72-of-organizations-remain-vulnerable-to-Log4Shell.

Warrick, J., & Nakashima, E. (2020, May 17). *Officials: Israel linked to a disruptive cyberattack on Iranian port facility*, The Washington Post. Retrieved November 29, 2023, from https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.

Weiss G. (2008). *The Farewell dossier: Duping the Soviets*, Central Intelligence Agency. Retrieved November 29, 2023, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm.

Weston, G. (2023, March 8). *IoT Connectivity Industry Forecast by 2030*, 101 blockchains. Retrieved November 29, 2023, from https://101blockchains.com/iot-connectivity-industry-forecast.

Whitman, M.E., & Mattord, H.J. (2012). *Principles of Information Security 4th edition*, Course Technology Cengage Learning, Boston.

Willsher, K. (2009). *French Fighter Planes Grounded by Computer Virus*, The Telegraph. Retrieved November 29, 2023, from http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

World Economic Forum. (2016, January 14). *The Fourth Industrial Revolution: what it means and how to respond*. Retrieved April 10, 2024, from https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.

World Economic Forum. (2018, April). Industrial Internet of Things Safety and Security Protocol, viewed 27 March 2024, from, https://www3.weforum.org/docs/47498_Industrial_Internet_Things_Safety_Security_Protocol_WP-FINAL.pdf.

Woolf, N. (2016, October 26). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. The Guardian. Retrieved November 29, 2023, from https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Wright, B. (2020, February 2). *Where is South Africa's industrial internet of things innovation?*, CIO. Retrieved November 29, 2023, from https://www.cio.com/article/201959/where-is-south-africas-industrial-internet-of-things-innovation.html.

Wu, H., Miao, Y., Zhang, P., Tian, Y., & Tian, H. (2022). Resilience in Industrial Internet of Things Systems: A Communication Perspective. arXiv preprint arXiv:2206.00217.

Wu, Y., Dai, H-N., Wang, H., Xiong, Z. & Guo, S. (2022, March 10). A Survey of Intelligent Network Slicing Management for Industrial IoT: Integrated Approaches for Smart Transportation, Smart Energy, and Smart Factory. In Secondquater 2022 *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, (pp. 1175-1211). doi: 10.1109/COMST.2022.3158270

Wyld, B. (2004). *The Fear Factor*, The Age. Retrieved November 29, 2023, from http://www.theage.com.au/articles/2004/07/16/1089694549469.html.

Yatagha, R., Waedt, K., Schindler, J., & Kirdan, E. (2023). Security challenges and best practices for resilient IIoT Networks: Network Segmentation.

Yin, R. (2009). Case study research: Design and methods. Los Angeles: Nelson Press.

Yu, K., Tan, L., Aloqaily, M., Yang, H., & Jararweh, Y. (2021). Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. *IEEE transactions on industrial informatics*, *17*(11), 7669-7678.

Zetter, L. (2015). *Is it Possible for Passengers to Hack Commercial Aircraft*, Wired. Retrieved November 29, 2023, from http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/.

Zimmerman, G. (2017). *Target Settles HVAC Data Breach for $18.5 Million*, Facilities Net. Retrieved November 29, 2023, from https://www.facilitiesnet.com/hvac/tip/Target-Settles-HVAC-Data-Breach-for-185-Million--39237.

Zurkus, K. (2019, June 27). *Silexbot Bricks Nearly 4000 IoT Devices*, Infosecurity Magazine. Retrieved November 29, 2023, from https://www.infosecurity-magazine.com/news/silexbot-bricks-nearly-4000-iot-1-1/.

Appendix A Questionnaire

Cybersecurity for Industrial Internet of Things: a case study of the South African transport sector

University of KwaZulu-Natal
School of Management, Information Technology and Governance

PhD Research Project

Researcher: Barend Pretorius (barend.pretorius@gmail.com)

Supervisor: Dr. Brett van Niekerk (VANNIEKERKB@ukzn.ac.za)
Co-Supervisor: Karunagaran Naidoo (naidook82@ukzn.ac.za)

Research Office: Ms. M Snyman (snymanm@ukzn.ac.za)

* Indicates required question

Informed Consent *

I, Barend Pretorius, a PhD student, at the School of Management, Information Technology and Governance, of the University of KwaZulu-Natal, invite you to participate in a research project entitled "Cybersecurity for Industrial Internet of Things: a case study of the South African transport sector". The aim of this study is to determine the status of Cybersecurity regarding IIoT and IoT (Threats, vulnerabilities, counter measures) and the factors influencing Cybersecurity related to IIoT and IoT in South Africa. The research will also aim to develop a South African framework specific to IIoT and IoT. Through your participation I hope to understand the status and the extent to which IIoT and IoT in the transportation sector of South Africa is being secured. The results of the survey are intended to contribute to my study and the South African Public sector in general. Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Management, Information Technology and Governance, UKZN. If you have any questions or concerns about completing the interview or about participating in this study, you may contact me or my supervisor at the email addresses listed above. This questionnaire should take about 10 minutes to complete. Sincerely Barend H. Pretorius

- ◯ I consent
- ◯ I DO NOT consent

Next

Page 1 of 7

Clear form

QUESTIONNAIRE

SECTION A: Demographics

A1. Type of Organization *

- ◯ NGO / NPO
- ◯ Public Organization
- ◯ Private Organization
- ◯ Other: _____

A2. Job Function *

- ◯ C-Level (CIO, CISO, CEO, CFO)
- ◯ Senior Management
- ◯ Management
- ◯ Operations
- ◯ Engineering
- ◯ Maintenance
- ◯ IT Administrator (System/Network/Database)
- ◯ Consultant
- ◯ Risk/Governance/Compliance
- ◯ Human Resources
- ◯ Analyst / technical (IT / Information Security / Business etc)
- ◯ Other: _____

A3. Number of Employees *

- ◯ Less than 100
- ◯ 100 - 1,000
- ◯ 1,001 - 5,000
- ◯ More than 5,000

A4. What is your primary interaction with IoT/IIoT *

- ◯ Governance / Risk / Compliance
- ◯ Security
- ◯ Audit / Consulting
- ◯ IT
- ◯ Engineering / Operations / OT
- ◯ Management of ICS/SCADA
- ◯ Vendor
- ◯ Academic research
- ◯ Some awareness of the risks / issues
- ◯ No knowledge of IoT/IIoT
- ◯ Other: _____

A5. How many years of experience with IoT/IIoT systems do you have? *

- ○ Less than 1 year
- ○ 1 - 2 years
- ○ 2 - 5 years
- ○ 5 - 10 years
- ○ 10 - 20 years
- ○ More than 20 years
- ○ None

A6. How many years of experience in the transport / logistics sector of South Africa? *

- ○ Less than 1 year
- ○ 1 - 2 years
- ○ 2 - 5 years
- ○ 5 - 10 years
- ○ 10 - 20 years
- ○ More than 20 years
- ○ No experience at all

Back Next Page 2 of 7 Clear form

SECTION B: Technology Factors influencing IoT/IIoT

B1. Existing and new threats introduced by IoT/IIoT *

Please rate the existing and new threats that IoT/IIoT would introduce in the transportation sector in South Africa. Note that there are 5 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

	No threat or not relevant	No change in threats	Slight increase in existing threats	IoT/IIoT increases existing threats	IoT/IIoT introduces new threats
Distributed Denial of Service (DDoS)	○	○	○	○	○
Insider and privilege misuse	○	○	○	○	○
Cyber espionage	○	○	○	○	○
Web Application attacks	○	○	○	○	○
Malware (worms / viruses / Trojans / spyware)	○	○	○	○	○
Natural disaster / environmental	○	○	○	○	○
Crime ware	○	○	○	○	○
Denial-of-sleep	○	○	○	○	○
Ransomware	○	○	○	○	○

Man-in-the-Middle attack	○	○	○	○	○
Remote access	○	○	○	○	○
Signal jamming attack	○	○	○	○	○
BlueBorne Attack (Bluetooth)	○	○	○	○	○
Other	○	○	○	○	○

If you know of any other threats actors not listed, please add them with their risk.

E.g. Strikes (IoT/IIoT introduces new threats)

Your answer

B2. Please select the top 3 threats related to your IoT/IIoT environment or an IoT/IIoT environment that you have encountered in the transportation sector in South Africa. *

Please only select 3.

- [ ] Distributed Denial of Service (DDoS)
- [ ] Insider and privilege misuse
- [ ] Cyber espionage
- [ ] Web application attacks
- [ ] Malware (worms / viruses / Trojans / spyware)
- [ ] Natural disaster / environmental
- [ ] Crime ware
- [ ] Denial-of-sleep
- [ ] Ransomware
- [ ] Man-in-the-Middle attack
- [ ] Remote access
- [ ] Signal jamming attack
- [ ] BlueBorne Attack (Bluetooth)
- [ ] Other: _____

B3. Vulnerabilities related to IoT/IIoT *

Please rate the vulnerabilities related to your IoT/IIoT environment or an IoT/IIoT environment that you have encountered in the transport sector in South Africa. Note that there are 5 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

	Very low	Low	Medium	High	Very high
No or weak password	○	○	○	○	○
No or delay in Patching / firmware updates	○	○	○	○	○
Misconfiguration	○	○	○	○	○
Weak or no encryption	○	○	○	○	○
Removable media	○	○	○	○	○
Insecure Default Settings	○	○	○	○	○
Weak or misconfigured protocols	○	○	○	○	○
Unreliable or insecure interfaces and APIs	○	○	○	○	○
Virus / malware (No software installed/unused/outdated)	○	○	○	○	○
Insecure wireless connections (overlooked and poorly configured)	○	○	○	○	○
Lack of Physical Hardening	○	○	○	○	○

Remote access – authentication not secure / shared passwords for vendors	○	○	○	○	○
Monitoring – No or limited	○	○	○	○	○
Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)	○	○	○	○	○
No privacy protection	○	○	○	○	○
Insecure Network Services	○	○	○	○	○
Use of insecure or outdated components	○	○	○	○	○
Insecure Data Transfer and Storage	○	○	○	○	○
Insecure Cloud interface	○	○	○	○	○
Insecure mobile interface	○	○	○	○	○

B4. Risks of unsecured IoT/IIoT devices (impact) *

Please rate the risk related to your IoT/IIoT environment or an IoT/IIoT environment that you have encountered in the transport sector in South Africa. Note that there are 5 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question. Insignificant (no impact on service/regulation) or Minor (Slight impact on service/regulation) or Moderate (Some service disruption/potential for adverse publicity) or Major (Service disruption/adverse publicity not avoidable) or Extreme/Catastrophic (Service interrupted for significant time/major adverse publicity not avoidable)

	Insignificant	Minor	Moderate	Major	Extreme/Catastrophic
Physical asset damage and associated loss of use	○	○	○	○	○
Unavailability of IoT/IIoT devices and/or networks	○	○	○	○	○
Loss or deletion of data	○	○	○	○	○
Data corruption or loss of data integrity	○	○	○	○	○
Data breach leading to the compromise of 3rd party confidential information, including personal information	○	○	○	○	○

Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information	○	○	○	○	○
Extortion demands to cease a cyber attack	○	○	○	○	○
Direct financial loss as a results of theft	○	○	○	○	○
Damage to reputation	○	○	○	○	○

B4. Risks of unsecured IoT/IIoT devices (likelihood) *

Please rate the likelihood of the risk related to your IoT/IIoT environment or an IoT/IIoT environment that you have encountered in the transport sector in South Africa occurring. Note that there are 5 options, depending on your web browser, you might have to scroll to the right via the scroll bar at the bottom of the question.

	Very low	Low	Medium	High	Very High
Physical asset damage and associated loss of use	○	○	○	○	○
Unavailability of IoT/IIoT devices and/or networks	○	○	○	○	○
Loss or deletion of data	○	○	○	○	○
Data corruption or loss of data integrity	○	○	○	○	○
Data breach leading to the compromise of 3rd party confidential information, including personal information	○	○	○	○	○

Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information	○	○	○	○	○
Extortion demands to cease a cyber attack	○	○	○	○	○
Direct financial loss as a results of theft	○	○	○	○	○
Damage to reputation	○	○	○	○	○

B5. Have any of the threats occurred in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

- ○ Yes
- ○ No
- ○ Maybe
- ○ Not sure
- ○ Can't disclose

B6. What type of IoT/IIoT or ICS/SCADA devices are in your organisation or an environment that you have encountered in the transport sector in South Africa? (Select all that apply) *

- [ ] Smart metering (e.g. energy monitoring)
- [ ] Boardroom / video conferencing
- [ ] Vehicle tracking / monitoring
- [ ] Cargo tracking
- [ ] ICS / SCADA
- [ ] Industrial controllers (e.g. PLCs)
- [ ] Cargo monitoring (e.g. reefer monitoring, status of cargo)
- [ ] Equipment monitoring
- [ ] Equipment tracking
- [ ] Industrial WiFi / LTE
- [ ] CCTV / smart cameras
- [ ] Building management systems (e.g. aircon controllers)
- [ ] Environmental monitoring (e.g. weather, wind, fire detections)
- [ ] Smart parking
- [ ] Traffic flow
- [ ] Sensors (General)
- [ ] Other: _____

Back Next Page 3 of 7 Clear form

SECTION C: Organisational factors

C1. Size and structure *

Rate the maturity for IoT/IIoT systems secured and governed in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa?

	No staff	Ad hoc staff	Allocated as part of a project	Part of daily tasks	Dedicated department dealing with it
Employees supporting IoT/IIoT	○	○	○	○	○
Security staff	○	○	○	○	○
IoT/IIoT security staff	○	○	○	○	○

C2. Security strategy *

Rate the maturity for each process in place for IoT/IIoT systems in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa?

	Initial (Process unpredictable, poorly controlled and reactive)	Managed (Process characterized for projects and is often reactive)	Defined (Processes characterized for the organization and is proactive)	Quantitatively Managed (Processes measured and controlled)	Focus on process improvement
Cybersecurity roadmap / strategy supporting IoT/IIoT	○	○	○	○	○
Risk assessment for IoT/IIoT	○	○	○	○	○
Governance processes for IoT/IIoT	○	○	○	○	○
Innovative culture in the organisation	○	○	○	○	○
Security culture in the organisation	○	○	○	○	○
Senior / Executive understanding of IoT/IIoT security risks	○	○	○	○	○

C3. Who do you believe is responsible for the security of IoT/IIoT in your organisation or an organisation you have encountered in the transport sector in South Africa? *

- ◯ Engineering/OT - They are in charge of the industrial control systems
- ◯ IT - They are in charge of the computer systems
- ◯ Security - They are in charge of securing our systems
- ◯ Lower management - They are in charge of implementing a culture of cybersecurity
- ◯ The Board - They are the decision-makers in terms of investment and creating a culture of security among employees
- ◯ All employees
- ◯ Not sure
- ◯ Other: _____

C4. Maturity of your security for your IoT/IIoT environment or an IoT/IIoT environment that you have encountered in the transport sector in South Africa. *

How do you perceive the maturity.

- ◯ 0 - None
- ◯ 1 - Basic (Very minimal or basic level of controls)
- ◯ 2 - Evolving (Inconsistently applied controls)
- ◯ 3 - Established (Controls in place, but there is a need for enhancement)
- ◯ 4 - Advanced (Control are consistently applied)
- ◯ 5 - Leading (Controls are established, consistently applied, regularly reviewed and coordinated)

Back Next Page 4 of 7 Clear form

SECTION D: Procedural factors

D1. Rate the maturity of incident response for IoT/IIoT systems secured and governed in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

Initial (Process unpredictable, poorly controlled and reactive) or Managed (Process characterized for projects and is often reactive) or Defined (Processes characterized for the organization and is proactive) or Quantitatively Managed (Processes measured and controlled) or Optimized (Focus on process improvement)

	Initial	Managed	Defined	Quantitatively Managed	Optimized	None / Not implemented
Organisation has a incident response plan	○	○	○	○	○	○
Incident response plan address IIoT risk	○	○	○	○	○	○

D2. Rate the maturity for IoT/IIoT policies, procedures, frameworks, standards, frameworks in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

Initial (Process unpredictable, poorly controlled and reactive) or Managed (Process characterized for projects and is often reactive) or Defined (Processes characterized for the organization and is proactive) or Quantitatively Managed (Processes measured and controlled) or Optimized (Focus on process improvement)

	Initial	Managed	Defined	Quantitatively Managed	Optimized	Nor impl
General security policies/procedures implemented	○	○	○	○	○	
IoT/IIoT security policies/procedures/controls implemented	○	○	○	○	○	
Governance processes for IoT/IIoT	○	○	○	○	○	
Control framework for IoT/IIoT	○	○	○	○	○	

D3. Standards/Control frameworks *

Please select all the control frameworks implemented/adopted for IoT/IIoT in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa?

- [ ] COBIT
- [ ] ISO27001
- [ ] NIST
- [ ] Online Trust Alliance
- [ ] Industrial Internet Consortium (IIC)
- [ ] Open Connectivity Foundation
- [ ] IEEE Internet of Things
- [ ] Alliance for Internet of Things Innovation
- [ ] Cloud Security Alliance
- [ ] Microsoft (Internet of Things security best practices)
- [ ] US Department of Homeland Security (DHS)
- [ ] Own developed
- [ ] Other: _____

If you have adopted or implemented any other standard / framework not listed, please add them.

E.g. ITIL

Your answer

D4. What type of intelligence do you rely on to detect threats aimed at your IoT/IIoT systems or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

Select all that apply.

- [ ] Rely on staff to know when to search out events
- [ ] Third-party intelligence provided
- [ ] Use anomaly detection tools (SIEM/SIC) to identify trends
- [ ] Review of audit logs
- [ ] None
- [ ] Other: _____

D5. How confident/certain are you that the implemented controls mitigating the threats and risks are sufficient for IoT/IIoT in the transport sector in South Africa? *

Select your confidence level.

- ◯ Not confident at all
- ◯ Some how confident
- ◯ Moderately confident
- ◯ Confident
- ◯ Very confident

D6. What are your top three priorities when it comes to implementing effective controls for the security of your IoT/IIoT systems or IoT/IIoT systems that you have encountered in the transport sector in South Africa? *

- [ ] Preventing harm to general public
- [ ] Protecting health and safety of employees
- [ ] Meeting regulatory compliance
- [ ] Securing connections to external systems
- [ ] Preventing control system service interruption
- [ ] Detecting/Enforcing control policy violations
- [ ] Preventing information leakage
- [ ] Lowering risk/Improving security
- [ ] Protecting company reputation and brand
- [ ] Preventing damage to systems
- [ ] Preventing financial loss/Protecting shareholder value
- [ ] Other: _____

D7. Rate the maturity of controls to protect against the risks imposed by new IoT/IIoT in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

Initial (Process unpredictable, poorly controlled and reactive) or Managed (Process characterized for projects and is often reactive) or Defined (Processes characterized for the organization and is proactive) or Quantitatively Managed (Processes measured and controlled) or Optimized (Focus on process improvement)

	Initial	Managed	Defined	Quantitatively Managed	Optimized	Non imple
Authentication/authorization	○	○	○	○	○	
System monitoring	○	○	○	○	○	
Encryption of communication	○	○	○	○	○	
SDLC for IoT/IIoT	○	○	○	○	○	
Segmentation (Firewall, standalone etc)	○	○	○	○	○	
Physical hardening	○	○	○	○	○	
Secure interfaces / API	○	○	○	○	○	
Secure protocols	○	○	○	○	○	
Regular and secure updates (Patching)	○	○	○	○	○	
Privacy protection (POPI, GDPR)	○	○	○	○	○	
Encryption of data	○	○	○	○	○	

Secure configuration (no default settings)	○	○	○	○	○

Back Next Page 5 of 7 Clear form

SECTION E: Human factors

E1. Rate the maturity of security awareness for IoT/IIoT systems secured and governed in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

Initial (Process unpredictable, poorly controlled and reactive) or Managed (Process characterized for projects and is often reactive) or Defined (Processes characterized for the organization and is proactive) or Quantitatively Managed (Processes measured and controlled) or Optimized (Focus on process improvement)

	Initial	Managed	Defined	Quantitatively Managed	Optimized	None / Not implemented
Security awareness in the organisation	○	○	○	○	○	○
Security awareness specific for IoT/IIoT	○	○	○	○	○	○

E2. Rate the maturity of skills for IoT/IIoT security skills in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

Initial (Process unpredictable, poorly controlled and reactive) or Managed (Process characterized for projects and is often reactive) or Defined (Processes characterized for the organization and is proactive) or Quantitatively Managed (Processes measured and controlled) or Optimized (Focus on process improvement)

	Initial	Managed	Defined	Quantitatively Managed	Optimized	None / Not implemented
Employees have general security skills	○	○	○	○	○	○
Employees have IoT/IIoT security skills	○	○	○	○	○	○
Employees are sufficiently trained to deal with IoT/IIoT security	○	○	○	○	○	○
The organisation enable staff for security	○	○	○	○	○	○

E3. Rate the maturity of employee engagement for IoT/IIoT security engagement in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

Initial (Process unpredictable, poorly controlled and reactive) or Managed (Process characterized for projects and is often reactive) or Defined (Processes characterized for the organization and is proactive) or Quantitatively Managed (Processes measured and controlled) or Optimized (Focus on process improvement)

	Initial	Managed	Defined	Quantitatively Managed	Optimized	None / Not implemented
Engineering/OT engagement with security staff	○	○	○	○	○	○
IT engagement with security staff	○	○	○	○	○	○
Management engagement with security staff	○	○	○	○	○	○
Executive management engagement with security staff	○	○	○	○	○	○

E4. Rate the maturity for IoT/IIoT employee satisfaction in your organisation or an IoT/IIoT environment that you have encountered in the transport sector in South Africa? *

Initial (Process unpredictable, poorly controlled and reactive) or Managed (Process characterized for projects and is often reactive) or Defined (Processes characterized for the organization and is proactive) or Quantitatively Managed (Processes measured and controlled) or Optimized (Focus on process improvement)

	Initial	Managed	Defined	Optimized	Strongly agree	None / Not implemented
Employees are satisfied with the oragnisation	○	○	○	○	○	○
The organisation provides the tools to manage IoT/IIoT security	○	○	○	○	○	○
Employees energy	○	○	○	○	○	○
Employees productivity	○	○	○	○	○	○

Back Next Page 6 of 7 Clear form

Cybersecurity for Industrial Internet of Things: a case study of the South African transport sector

barend.pretorius@gmail.com Switch accounts

Not shared

Thank you for completing the survey!

If you would like to receive the feedback results, please leave your email address below:

Your answer

Back Submit Page 7 of 7 Clear form

Appendix B Additional Tables

Table B1: Correlation table between Technological (Threats) and Organisational Factors

	DDoS	Insider and privilege misuse	Cyber espionage	Web Application attacks	Malware	Natural disaster / environmental	Crime ware	Denial-of-sleep	Ransomware	Man-in-the-Middle attack	Remote access	Signal jamming attack	BlueBorne Attack (Bluetooth)	Other
Employees supporting IIoT	-0.2	0.0	-0.2	-0.1	0.0	0.1	-0.1	-0.1	-0.1	-0.2	0.0	0.0	-0.1	0.2
Size and structure [Security staff]	-0.3	-0.1	-0.3	-0.1	0.0	0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	-0.1	0.0
Size and structure [IIoT security staff]	-0.4	-0.2	-0.1	-0.2	-0.2	0.0	-0.2	-0.2	-0.3	-0.3	-0.3	-0.2	-0.1	0.0
Security strategy	-0.3	-0.2	-0.2	-0.2	-0.2	0.0	-0.1	-0.3	-0.3	-0.4	-0.3	-0.2	-0.1	0.0
Risk assessment for IIoT	-0.4	-0.2	-0.5	-0.2	-0.1	-0.1	-0.2	-0.5	-0.3	-0.4	-0.3	-0.4	-0.3	-0.1
Governance processes for IIoT	-0.5	-0.3	-0.5	-0.4	-0.3	-0.2	-0.3	-0.4	-0.5	-0.5	-0.5	-0.5	-0.4	-0.3
Innovative culture in the organisation	-0.3	-0.1	-0.4	-0.1	-0.1	0.1	-0.1	-0.3	-0.1	-0.3	-0.2	-0.3	-0.2	0.0
Security culture in the organisation	-0.4	-0.1	-0.3	-0.2	-0.2	-0.1	-0.2	-0.3	-0.2	-0.5	-0.3	-0.4	-0.3	-0.1
Senior / Executive understanding of IIoT security risks	-0.4	-0.1	-0.4	-0.2	-0.1	0.0	-0.2	-0.4	-0.2	-0.3	-0.3	-0.4	-0.3	-0.1

Table B2: Correlation table between Technological (Vulnerabilities) and Organisational Factors

	No or weak password	No or delay in Patching / firmware updates	Misconfiguration	Weak or no encryption	Removable media	Insecure Default Settings	Weak or misconfigured protocols	Unreliable or insecure interfaces and APIs	Virus / malware (No software installed/unused/outdated)	Insecure wireless connections (overlooked and poorly configured)
Employees supporting IIoT	0.2	0.2	0.2	0.3	0.2	0.3	0.3	0.2	0.2	0.2
Size and structure [Security staff]	0.1	-0.1	0.0	0.2	0.0	0.2	0.1	0.1	0.1	0.0
Size and structure [IIoT security staff]	0.0	-0.2	0.0	0.0	0.0	0.1	0.0	0.2	-0.1	0.0
Security strategy [Cybersecurity roadmap / strategy supporting IIoT]	0.2	0.0	0.1	0.0	0.0	0.1	0.1	0.1	-0.1	0.0
Risk assessment for IIoT	0.2	0.0	0.0	0.0	0.0	0.1	0.1	0.0	0.0	0.0
Governance processes for IIoT	0.2	-0.1	-0.2	-0.2	0.0	-0.1	0.0	-0.1	0.0	-0.2
Innovative culture in the organisation	0.3	0.1	0.0	0.1	0.1	0.1	0.1	0.0	0.0	0.0
Security culture in the organisation	0.1	-0.1	-0.1	-0.1	-0.1	0.0	0.0	0.0	0.0	-0.1
Senior / Executive understanding of IIoT security risks	0.3	0.0	0.0	0.0	-0.2	0.0	0.0	0.0	-0.1	0.0

Table B3: Correlation table between Technological (Vulnerabilities) and Organisational Factors

	Lack of Physical Hardening	Remote access – authentication not secure / shared passwords for vendors	Monitoring – No or limited	Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)	No privacy protection	Insecure Network Services	Use of insecure or outdated components	Insecure Data Transfer and Storage	Insecure Cloud interface	Insecure mobile interface
Employees supporting IIoT	0.1	0.2	0.1	0.2	0.2	0.2	0.3	0.2	0.1	0.1
Size and structure [Security staff]	-0.1	0.0	0.0	0.1	0.2	0.1	0.2	0.0	0.0	0.0
Size and structure [IIoT security staff]	0.0	-0.1	-0.1	0.1	0.1	0.1	0.0	-0.1	0.1	0.1
Security strategy [Cybersecurity roadmap / strategy supporting IIoT]	0.1	0.0	0.0	0.2	0.2	0.1	0.0	0.1	0.1	0.1
Risk assessment for IIoT	0.0	0.0	0.0	-0.1	0.1	0.1	0.0	0.1	-0.1	-0.1
Governance processes for IIoT	-0.1	-0.1	-0.2	-0.1	-0.1	-0.1	-0.1	-0.1	-0.2	-0.2
Innovative culture in the organisation	0.0	0.0	0.1	-0.1	0.0	0.0	0.2	0.1	-0.1	-0.1
Security culture in the organisation	-0.1	-0.1	-0.1	-0.2	-0.1	-0.1	0.0	0.0	-0.1	-0.2
Senior / Executive understanding of IIoT security risks	0.0	0.0	0.0	-0.2	0.0	0.1	0.2	0.0	-0.1	-0.2

Table B4: Correlation table between Technological (Risk Impact) and Organisational Factors

	Risks (Impact)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Employees supporting IIoT	0.1	0.1	0.1	0.1	0.0	0.0	-0.1	0.0	-0.1
Size and structure [Security staff]	0.0	0.0	0.1	0.1	0.0	-0.1	0.1	0.1	0.0
Size and structure [IIoT security staff]	0.0	0.2	0.0	0.0	0.0	0.1	0.1	0.1	0.0
Security strategy [Cybersecurity roadmap / strategy supporting IIoT]	-0.1	0.2	-0.1	0.0	0.0	0.1	0.0	0.0	0.0
Risk assessment for IIoT	0.0	0.1	0.1	0.0	0.0	-0.1	-0.1	-0.2	-0.2
Governance processes for IIoT	-0.1	0.0	0.0	0.0	0.0	-0.1	-0.1	0.0	-0.1
Innovative culture in the organisation	0.0	0.1	0.1	0.0	0.0	-0.1	-0.1	-0.1	-0.1
Security culture in the organisation	-0.2	0.0	0.0	0.0	0.0	-0.1	0.0	-0.1	-0.1
Senior / Executive understanding of IIoT security risks	-0.1	0.1	0.1	0.0	0.0	0.0	0.0	0.0	0.0

Table B5: Correlation table between Technological (Risk likelihood) and Organisational Factors

	Risks (Likelihood)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Employees supporting IIoT	0.1	0.1	0.1	0.0	0.1	0.0	0.0	0.0	0.0
Size and structure [Security staff]	0.0	0.0	0.1	0.1	0.1	-0.1	0.0	0.0	0.0
Size and structure [IIoT security staff]	-0.1	0.0	0.0	0.0	0.0	0.2	0.1	0.2	0.1
Security strategy [Cybersecurity roadmap / strategy supporting IIoT]	0.0	0.0	0.0	0.0	0.0	0.1	0.0	0.1	0.1
Risk assessment for IIoT	-0.1	0.1	0.1	0.1	0.1	-0.1	-0.1	-0.1	-0.1
Governance processes for IIoT	-0.2	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0
Innovative culture in the organisation	-0.1	0.1	0.2	0.1	0.1	0.0	0.0	-0.1	-0.1
Security culture in the organisation	-0.3	-0.1	0.0	-0.1	0.0	0.0	0.0	-0.1	0.0
Senior / Executive understanding of IIoT security risks	-0.1	0.1	0.2	0.1	0.1	0.0	0.0	0.0	0.1

Table B6: Correlation table between Technological (Vulnerabilities) and Procedural Factors

	Vulnerabilities									
	No or weak password	*No or delay in Patching / firmware updates*	*Misconfiguration*	*Weak or no encryption*	*Removable media*	*Insecure Default Settings*	*Weak or misconfigured protocols*	*Unreliable or insecure interfaces and APIs*	*Virus / malware (No software installed/unused/outdated)*	*Insecure wireless connections (overlooked and poorly configured)*
Organisation has an incident response plan	0.2	0.1	0.1	0.3	0.1	0.3	0.3	0.3	0.1	0.1
Incident response plan address IIoT risk	0.0	0.0	-0.2	0.0	-0.1	0.0	0.0	0.0	0.1	0.0
Risk assessment for IIoT	0.2	0.0	0.0	0.0	0.0	0.1	0.1	0.0	0.0	0.0
General security policies/ procedures implemented	-0.1	-0.1	-0.1	0.1	0.1	0.0	0.0	0.0	0.0	-0.1
IIoT security policies/ procedures/controls implemented	-0.1	-0.2	-0.2	-0.2	-0.2	-0.3	-0.3	-0.1	0.0	-0.2
Governance processes for IIoT	-0.1	-0.2	-0.3	-0.3	-0.1	-0.2	-0.2	-0.1	-0.1	-0.1
Control framework for IIoT	-0.1	-0.2	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.1	-0.2

Table B7: Correlation table between Technological (Vulnerabilities) and Procedural Factors (Cont'd)

	Vulnerabilities (cont'd)									
	Lack of Physical Hardening	Remote access – authentication not secure / shared passwords for vendors	Monitoring – No or limited	Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)	No privacy protection	Insecure Network Services	Use of insecure or outdated components	Insecure Data Transfer and Storage	Insecure Cloud interface	Insecure mobile interface
Organisation has an incident response plan	0.0	0.2	0.0	0.2	0.3	0.3	0.4	0.3	0.2	0.1
Incident response plan address IIoT risk	-0.2	0.0	-0.1	-0.1	0.1	0.1	0.2	0.2	0.0	0.0
Risk assessment for IIoT	0.0	0.0	0.0	-0.1	0.1	0.1	0.0	0.1	-0.1	-0.1
General security policies/ procedures implemented	-0.1	-0.1	-0.2	0.1	0.0	0.0	-0.1	0.0	0.2	0.1
IIoT security policies/ procedures/controls implemented	-0.2	-0.3	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	0.0	0.0
Governance processes for IIoT	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.2	0.0	0.1	0.1
Control framework for IIoT	-0.2	-0.2	-0.2	-0.1	-0.1	-0.1	-0.2	0.0	0.0	0.0

Table B8: Correlation table between Technological (Risk Impact) and Procedural Factors

	Risks (Impact)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Organisation has an incident response plan	0.0	0.2	0.2	0.2	0.1	0.1	0.1	0.0	0.0
Incident response plan address IIoT risk	-0.1	0.1	0.1	0.0	0.0	-0.1	-0.1	-0.2	-0.2
Risk assessment for IIoT	0.0	0.1	0.1	0.0	0.0	-0.1	-0.1	-0.2	-0.2
General security policies/ procedures implemented	-0.2	0.1	0.0	-0.1	0.0	0.1	0.0	0.0	0.0
IIoT security policies/ procedures/controls implemented	-0.3	0.0	-0.1	0.0	0.0	0.0	0.0	0.0	-0.1
Governance processes for IIoT	-0.2	0.1	-0.1	-0.1	0.0	0.0	-0.1	-0.2	-0.1
Control framework for IIoT	-0.3	0.0	-0.2	-0.1	-0.1	0.0	-0.1	-0.1	-0.1

Table B9: Correlation table between Technological (Risk Likelihood) and Procedural Factors

	Risks (Likelihood)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Organisation has an incident response plan	0.2	0.2	0.3	0.3	0.2	0.1	0.2	0.2	0.2
Incident response plan address IIoT risk	-0.1	0.1	0.0	0.0	-0.1	-0.2	-0.2	-0.1	-0.1
Risk assessment for IIoT	-0.1	0.1	0.1	0.1	0.1	-0.1	-0.1	-0.1	-0.1
General security policies/ procedures implemented	-0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1
IIoT security policies/ procedures/controls implemented	-0.3	-0.1	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1	0.0
Governance processes for IIoT	-0.2	0.0	-0.1	-0.2	-0.2	-0.1	-0.2	-0.1	-0.1
Control framework for IIoT	-0.2	-0.1	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1

Table B10: Correlation table between Technological (Threats) and People Factors

	Threats													
	DDoS	Insider and privilege misuse	Cyber espionage	Web Application attacks	Malware	Natural disaster / environmental	Crime ware	Denial-of-sleep	Ransomware	Man-in-the-Middle attack	Remote access	Signal jamming attack	BlueBorne Attack (Bluetooth)	Other
Security awareness in the organisation	0.0	0.0	0.2	0.1	0.1	0.1	0.0	0.1	0.1	0.0	0.1	0.1	0.3	-0.1
Security awareness specific for IIoT	-0.1	0.0	-0.1	-0.1	-0.1	0.0	-0.1	-0.2	-0.1	-0.1	-0.2	-0.2	-0.1	0.0
Employees have general security skills	0.2	0.0	0.2	0.0	0.1	0.0	0.0	0.1	0.2	0.1	0.1	0.0	0.2	0.0
Employees have IIoT security skills	0.0	0.0	0.0	-0.1	0.0	0.0	0.0	-0.2	-0.1	0.0	-0.1	-0.2	-0.1	0.0
Employees are sufficiently trained to deal with IIoT security	0.0	0.0	-0.1	0.0	0.0	0.1	0.0	-0.2	0.0	0.0	-0.1	-0.1	0.0	0.0
The organisation enable staff for security	0.1	0.1	0.1	0.1	0.2	0.2	0.2	0.1	0.2	0.1	0.1	0.0	0.2	0.1
Engineering/ OT engagement with security staff	0.0	0.0	-0.1	-0.1	0.0	0.0	-0.2	-0.2	0.0	0.0	-0.1	-0.2	0.0	-0.1
IT engagement with security staff	-0.2	0.0	-0.2	-0.1	0.1	-0.1	-0.1	-0.2	0.0	0.0	0.0	-0.2	0.0	-0.2
Management engagement with security staff	-0.1	0.1	-0.1	0.1	0.2	0.2	0.1	-0.1	0.2	0.1	0.1	-0.2	0.0	0.0
Executive management engagement	0.0	0.0	0.0	0.0	0.0	0.2	0.0	0.0	0.2	0.0	0.0	0.0	0.2	0.0

	Threats													
	DDoS	Insider and privilege misuse	Cyber espionage	Web Application attacks	Malware	Natural disaster / environmental	Crime ware	Denial-of-sleep	Ransomware	Man-in-the-Middle attack	Remote access	Signal jamming attack	BlueBorne Attack (Bluetooth)	Other
with security staff														
Employees are satisfied with the organisation	0.1	0.0	0.0	0.2	0.1	0.3	0.1	0.0	0.2	0.0	0.1	0.0	0.2	-0.1
The organisation provides the tools to manage IIoT security	-0.2	-0.1	-0.1	0.0	0.0	0.1	-0.2	-0.1	0.1	-0.2	0.0	-0.1	0.0	0.0
Employee's energy	0.0	0.0	0.0	0.2	0.2	0.3	0.1	0.0	0.2	0.1	0.1	0.0	0.1	0.0
Employee's productivity	0.0	0.1	0.1	0.1	0.2	0.2	0.1	-0.1	0.1	0.0	0.1	0.0	0.2	0.2

Table B11: Correlation table between Technological (Vulnerabilities) and People Factors

	Vulnerabilities									
	No or weak password	No or delay in Patching / firmware updates	Misconfiguration	Weak or no encryption	Removable media	Insecure Default Settings	Weak or misconfigured protocols	Unreliable or insecure interfaces and APIs	Virus / malware (No software installed/unused/outdated)	Insecure wireless connections (overlooked and poorly configured)
Security awareness in the organisation	0.1	0.0	0.2	0.1	-0.1	0.1	0.1	0.1	0.0	0.1
Security awareness specific for IIoT	-0.1	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.3	-0.2	-0.3

	Vulnerabilities									
	No or weak password	**No or delay in Patching / firmware updates**	**Misconfiguration**	**Weak or no encryption**	**Removable media**	**Insecure Default Settings**	**Weak or misconfigured protocols**	**Unreliable or insecure interfaces and APIs**	**Virus / malware (No software installed/unused/outdated)**	**Insecure wireless connections (overlooked and poorly configured)**
Employees have general security skills	0.0	0.0	0.0	0.2	0.0	0.1	0.1	-0.1	0.0	0.1
Employees have IIoT security skills	-0.1	-0.3	-0.4	-0.2	-0.3	-0.2	-0.3	-0.3	-0.2	-0.2
Employees are sufficiently trained to deal with IIoT security	-0.1	-0.3	-0.4	-0.2	-0.3	-0.2	-0.2	-0.3	-0.2	-0.2
The organisation enable staff for security	0.1	-0.1	-0.1	0.0	-0.1	0.0	0.0	-0.1	-0.1	0.0
Engineering/OT engagement with security staff	0.0	-0.2	-0.2	-0.1	-0.2	-0.1	-0.2	-0.2	-0.2	-0.2
IT engagement with security staff	0.0	-0.1	-0.1	0.1	-0.2	0.0	0.0	-0.1	0.0	0.0
Management engagement with security staff	0.1	-0.1	-0.1	0.1	0.0	0.0	0.0	0.0	0.0	0.0
Executive management engagement with security staff	0.1	0.0	0.0	0.1	-0.1	0.0	0.0	0.0	-0.1	0.0
Employees are satisfied with the organisation	0.1	0.0	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.1
The organisation provides the tools to manage IIoT security	0.0	-0.2	-0.1	0.0	-0.1	-0.2	-0.1	-0.1	-0.1	0.0
Employee's energy	-0.1	-0.2	-0.1	0.0	-0.1	-0.1	0.0	-0.1	0.0	0.0
Employee's productivity	0.0	-0.1	0.0	0.1	-0.1	0.0	-0.1	0.0	0.0	0.1

Table B12: Correlation table between Technological (Vulnerabilities) and People Factors

	Vulnerabilities (cont'd)									
	Lack of Physical Hardening	**Remote access – authentication not secure / shared passwords for vendors**	**Monitoring – No or limited**	**Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)**	**No privacy protection**	**Insecure Network Services**	**Use of insecure or outdated components**	**Insecure Data Transfer and Storage**	**Insecure Cloud interface**	**Insecure mobile interface**
Security awareness in the organisation	0.1	0.0	-0.1	0.0	0.0	0.1	0.2	0.0	0.1	0.0
Security awareness specific for IIoT	-0.3	-0.2	-0.3	-0.2	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2
Employees have general security skills	-0.1	0.0	0.0	0.1	0.1	0.1	0.1	0.1	0.1	0.0
Employees have IIoT security skills	-0.3	-0.3	-0.2	-0.2	-0.1	-0.2	-0.3	-0.3	-0.2	-0.2
Employees are sufficiently trained to deal with IIoT security	-0.3	-0.3	-0.3	-0.2	-0.2	-0.2	-0.2	-0.2	-0.1	-0.1
The organisation enable staff for security	-0.2	-0.1	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0
Engineering/OT engagement with security staff	-0.2	-0.2	-0.2	-0.1	0.0	-0.1	0.0	-0.1	-0.2	-0.2
IT engagement with security staff	-0.2	0.1	-0.1	0.0	0.1	0.2	0.1	0.0	-0.1	-0.1

	Vulnerabilities (cont'd)									
	Lack of Physical Hardening	**Remote access – authentication not secure / shared passwords for vendors**	**Monitoring – No or limited**	**Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)**	**No privacy protection**	**Insecure Network Services**	**Use of insecure or outdated components**	**Insecure Data Transfer and Storage**	**Insecure Cloud interface**	**Insecure mobile interface**
Management engagement with security staff	-0.3	0.0	-0.1	0.0	0.1	0.1	0.2	0.1	0.0	-0.1
Executive management engagement with security staff	-0.2	-0.1	-0.2	0.1	0.1	0.1	0.1	0.0	0.2	0.1
Employees are satisfied with the organisation	-0.2	-0.1	-0.2	0.1	0.0	-0.1	0.1	0.0	0.0	-0.1
The organisation provides the tools to manage IIoT security	-0.3	-0.2	-0.2	-0.1	-0.2	-0.1	0.0	-0.1	-0.2	-0.2
Employee's energy	-0.4	-0.1	-0.2	0.1	0.0	0.0	0.0	0.0	0.0	-0.1
Employee's productivity	-0.3	-0.2	-0.1	0.1	0.0	0.0	0.0	0.0	0.0	0.0

Table B13: Correlation table between Technological (Risk Impact) and People Factors

	Risks (Impact)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Security awareness in the organisation	0.0	0.2	0.1	0.0	0.0	0.0	0.0	0.1	0.0
Security awareness specific for IIoT	0.0	0.0	-0.1	-0.1	-0.1	-0.1	-0.1	0.0	-0.1
Employees have general security skills	0.0	0.1	0.1	0.0	0.0	0.1	0.0	0.1	0.1
Employees have IIoT security skills	-0.1	-0.1	-0.2	-0.1	-0.2	-0.1	-0.1	0.0	0.0
Employees are sufficiently trained to deal with IIoT security	-0.1	0.0	-0.1	-0.1	-0.1	0.0	-0.1	0.0	0.0
The organisation enable staff for security	0.0	0.0	-0.1	-0.1	-0.1	0.0	0.0	0.0	0.1
Engineering/OT engagement with security staff	0.0	-0.1	-0.1	-0.1	-0.1	-0.1	-0.2	-0.1	-0.1
IT engagement with security staff	0.0	-0.1	0.1	0.1	0.1	0.0	-0.1	0.0	0.0
Management	0.0	0.0	0.2	0.1	0.1	0.1	0.1	0.0	0.0

	Risks (Impact)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
engagement with security staff									
Executive management engagement with security staff	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Employees are satisfied with the organisation	0.0	0.1	0.1	0.0	0.0	0.1	-0.1	0.0	-0.1
The organisation provides the tools to manage IIoT security	0.0	0.0	0.0	0.0	0.0	0.0	-0.1	0.0	-0.1
Employee's energy	0.0	0.1	0.1	0.1	0.1	0.1	0.0	0.0	-0.1
Employee's productivity	0.0	0.2	0.1	0.0	0.1	0.1	0.0	0.1	0.0

Table B14: Correlation table between Technological (Risk Likelihood) and People Factors

	Risks (Likelihood)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Security awareness in the organisation	0.0	-0.1	0.0	0.0	0.0	0.0	0.1	0.1	0.1
Security awareness specific for IIoT	-0.2	-0.1	-0.1	-0.1	-0.1	0.0	0.0	0.0	0.0
Employees have general security skills	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1
Employees have IIoT security skills	-0.1	-0.1	0.0	0.0	-0.1	-0.2	-0.2	0.0	0.0
Employees are sufficiently trained to deal with IIoT security	-0.1	0.0	0.0	0.0	0.0	-0.1	-0.1	0.1	0.1
The organisation enable	0.0	0.0	0.0	0.0	0.1	0.0	0.0	0.2	0.1

	Risks (Likelihood)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
staff for security									
Engineering/OT engagement with security staff	-0.1	-0.1	-0.1	-0.1	-0.1	-0.2	-0.1	0.0	0.1
IT engagement with security staff	-0.1	-0.1	0.0	0.0	0.1	-0.2	-0.1	-0.1	0.1
Management engagement with security staff	0.0	0.1	0.2	0.2	0.3	0.0	0.1	0.1	0.1
Executive management engagement with security staff	0.1	0.0	0.1	0.2	0.2	0.2	0.1	0.2	0.3
Employees are satisfied with the organisation	-0.1	0.0	0.1	0.1	0.1	0.1	0.1	0.1	0.2
The organisation provides the tools to manage IIoT security	-0.2	-0.1	-0.1	-0.1	0.0	-0.1	0.0	0.1	0.0
Employee's energy	-0.1	-0.1	0.0	0.0	0.0	0.0	0.1	0.1	0.1

	Risks (Likelihood)								
	Physical asset damage and associated loss of use	**Unavailability of IIoT devices or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyberattack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Employee's productivity	0.0	0.0	0.0	0.0	0.1	0.0	0.1	0.1	0.1

Appendix C Additional Word Trees

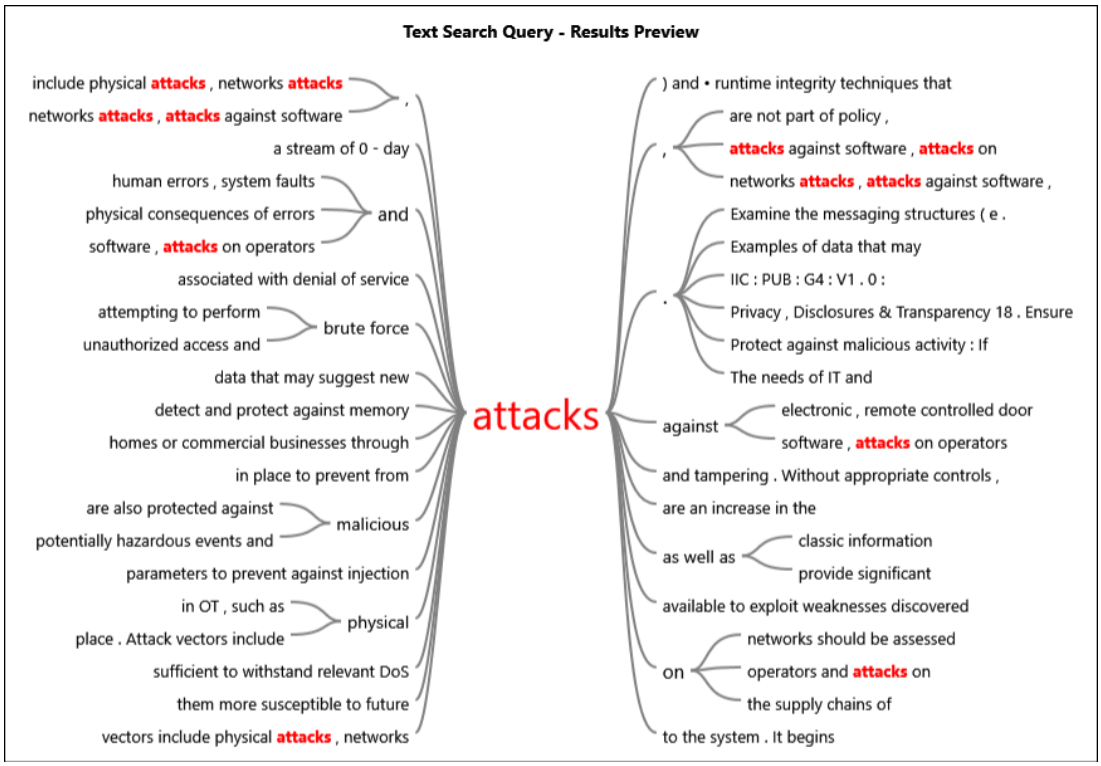


Figure C1: Word tree for 'attacks' under the threat node

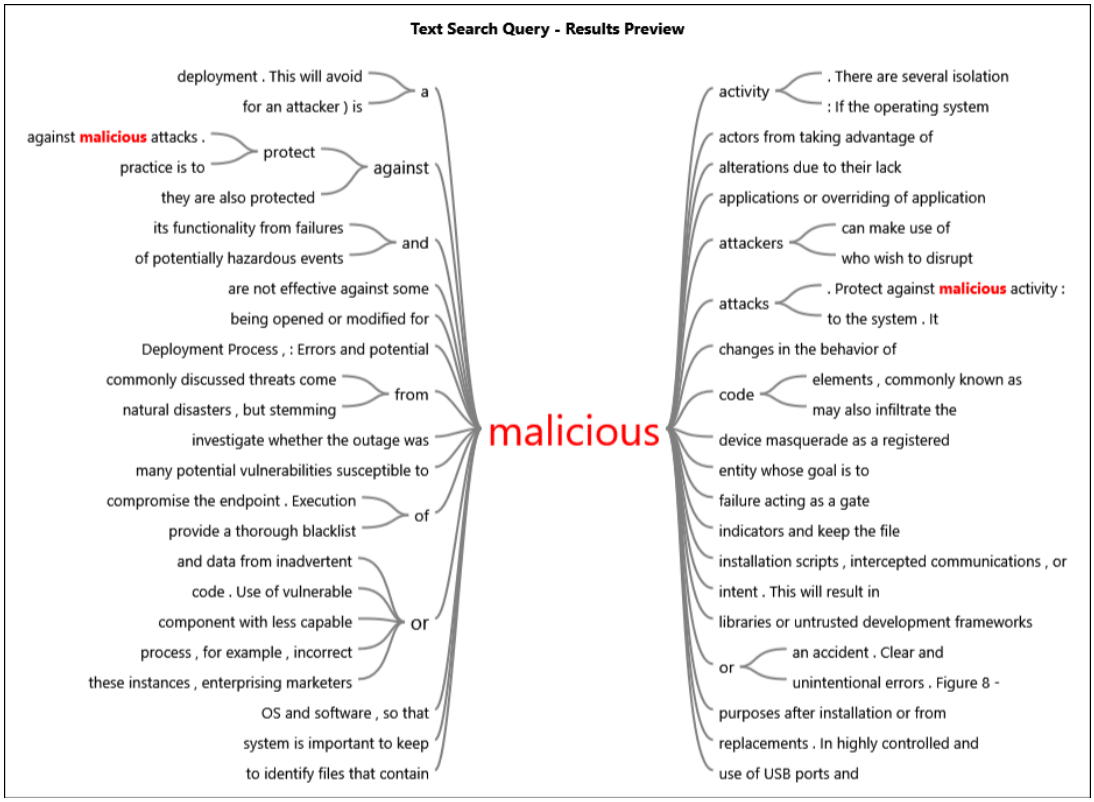


Figure C2: Word tree for 'malicious' under the threat node

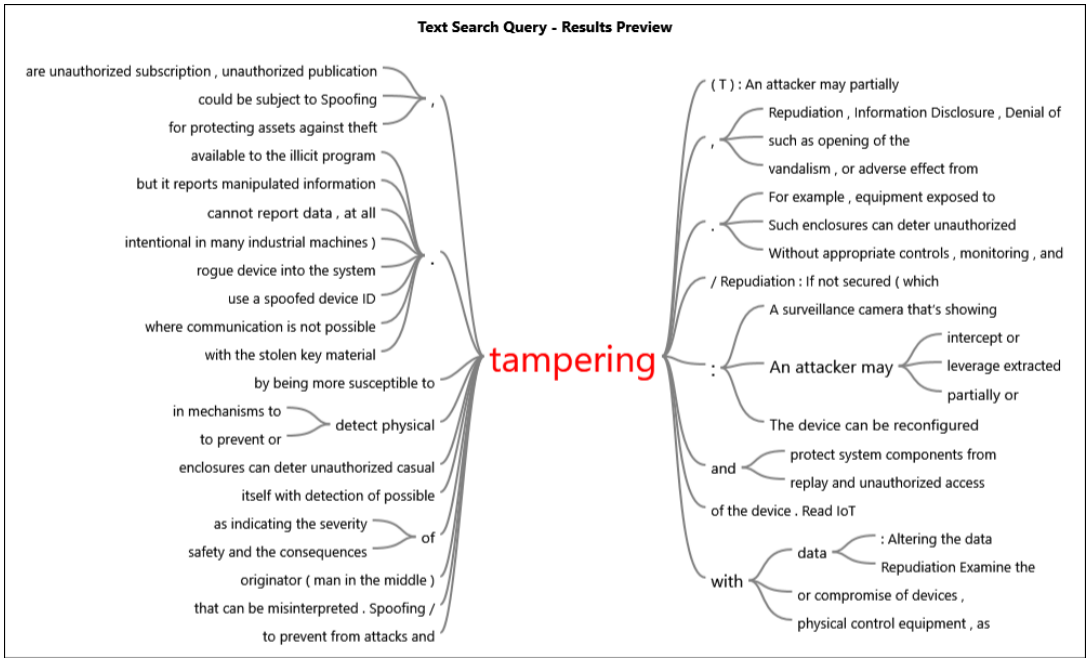


Figure C3: Word tree for 'tampering' under the threat node

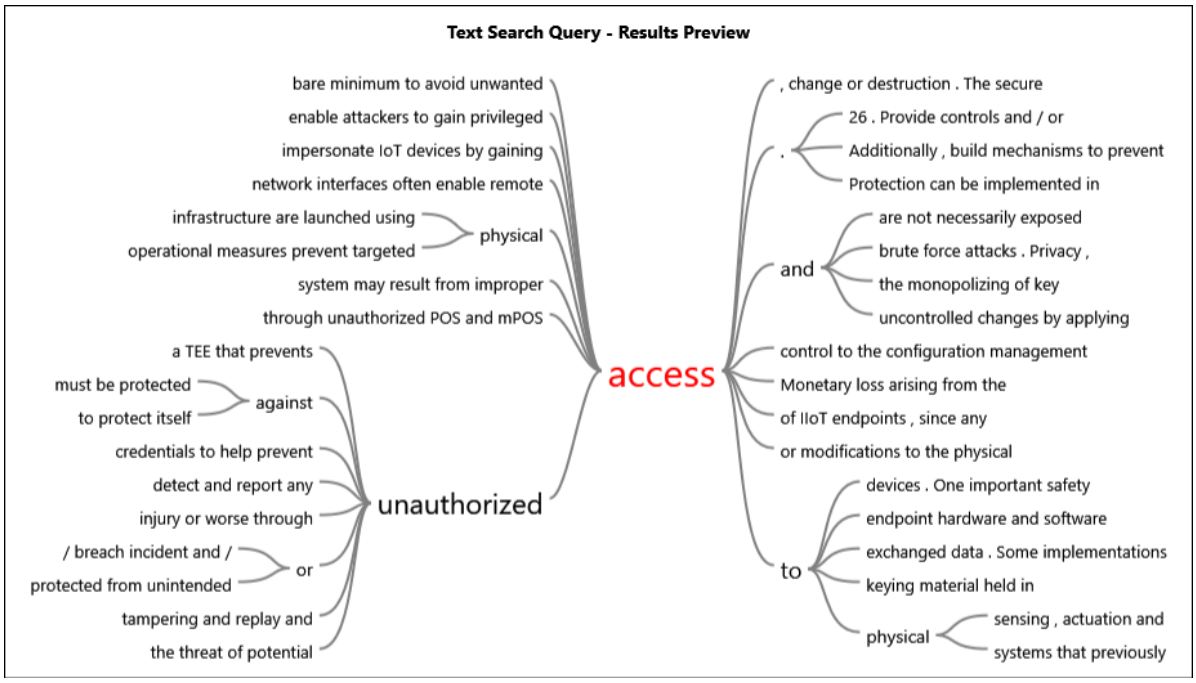


Figure C4: Word tree for 'access' under the threat node

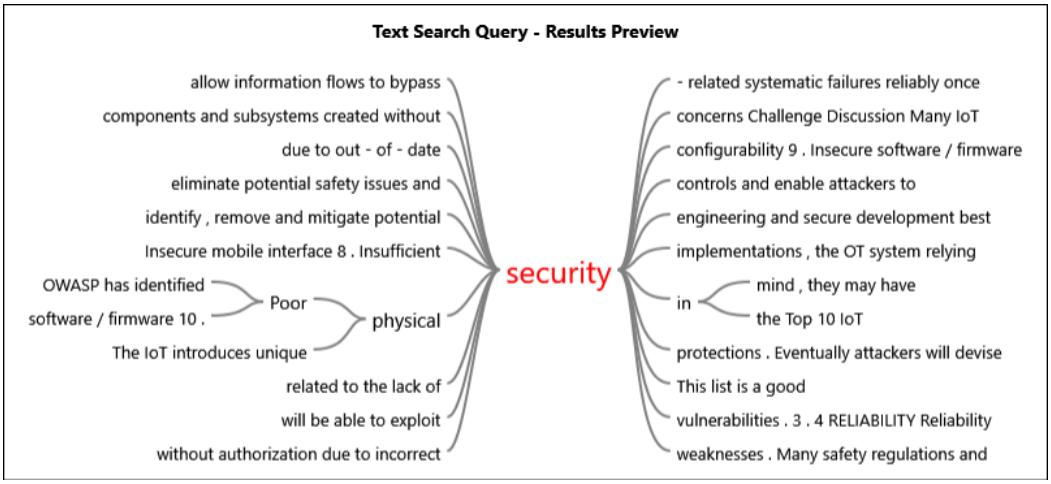


Figure C5: Word tree for 'security' under the vulnerability node

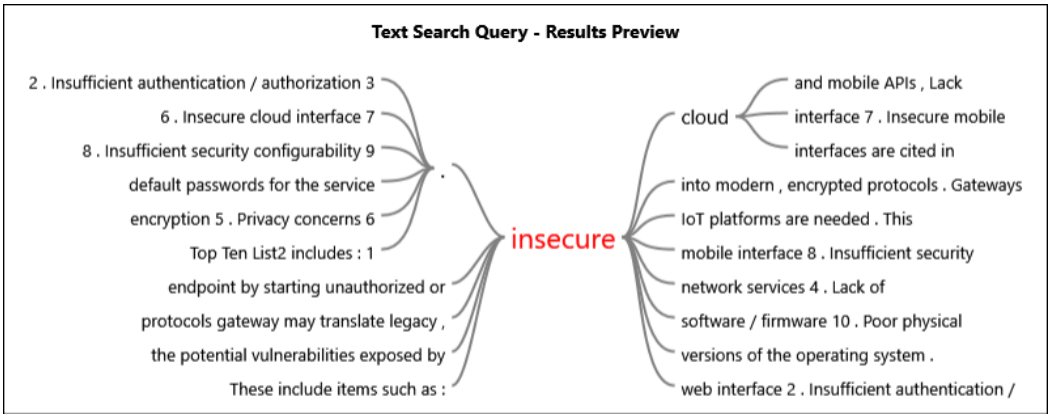


Figure C6: Word tree for 'insecure' under the vulnerability node

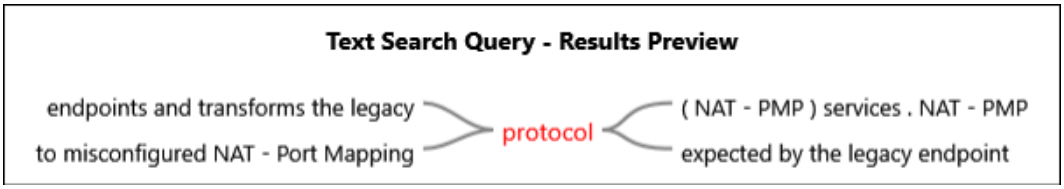


Figure C7: Word tree for 'protocol' under the vulnerability node

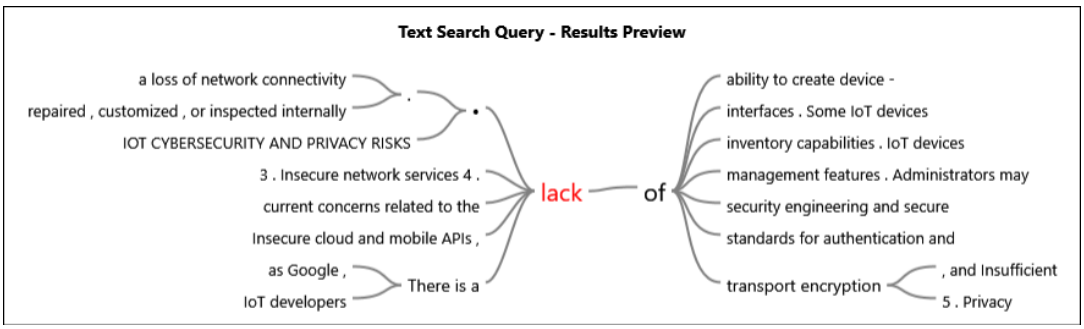


Figure C8: Word tree for 'lack' under the vulnerability node

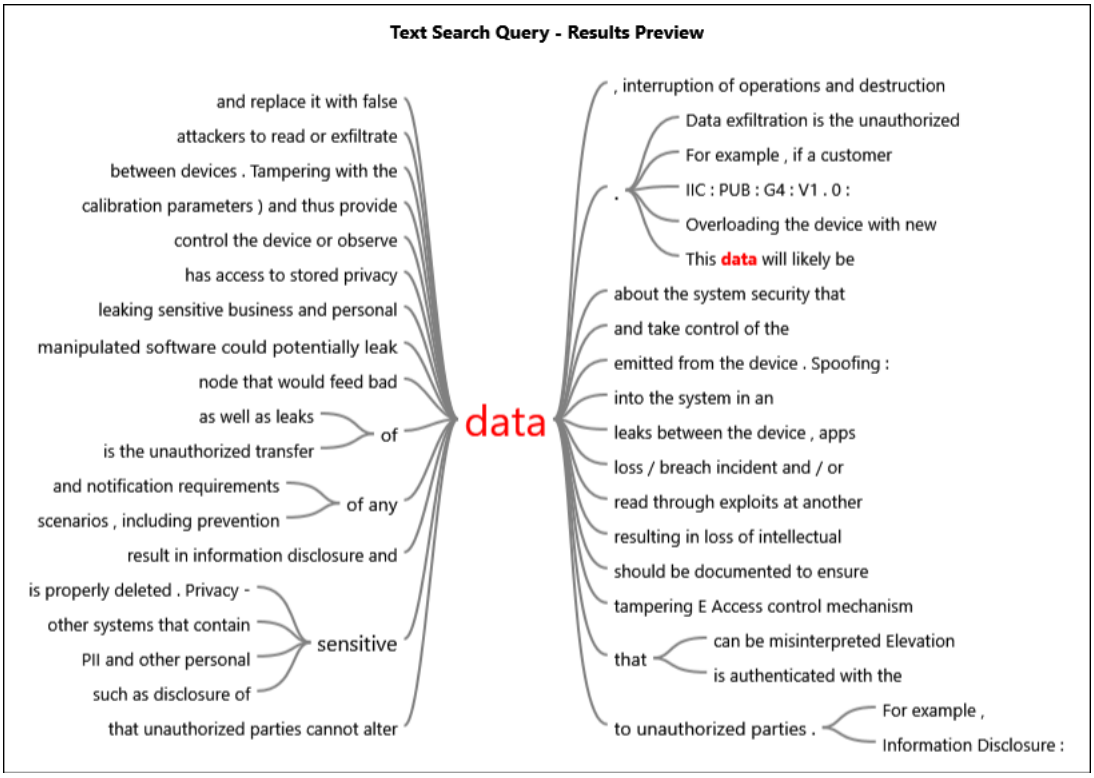


Figure C9: Word tree for 'data' under the risk node

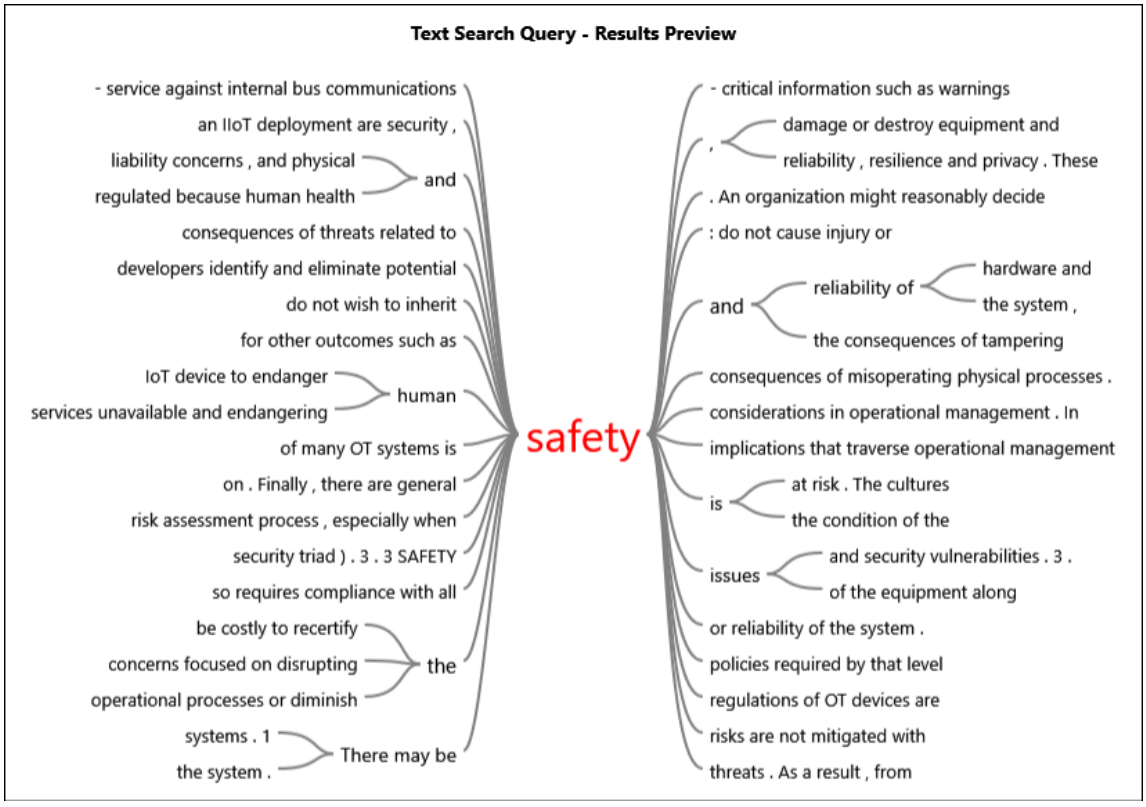


Figure C10: Word tree for 'safety' under the risk node

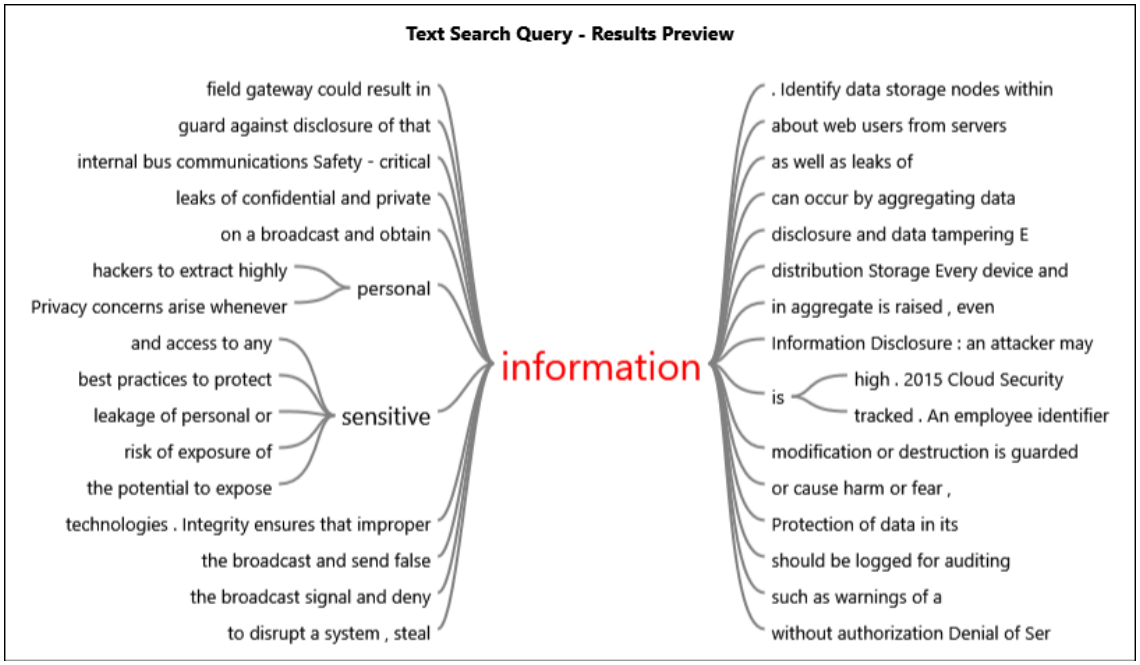


Figure C11: Word tree for 'information' under the risk node

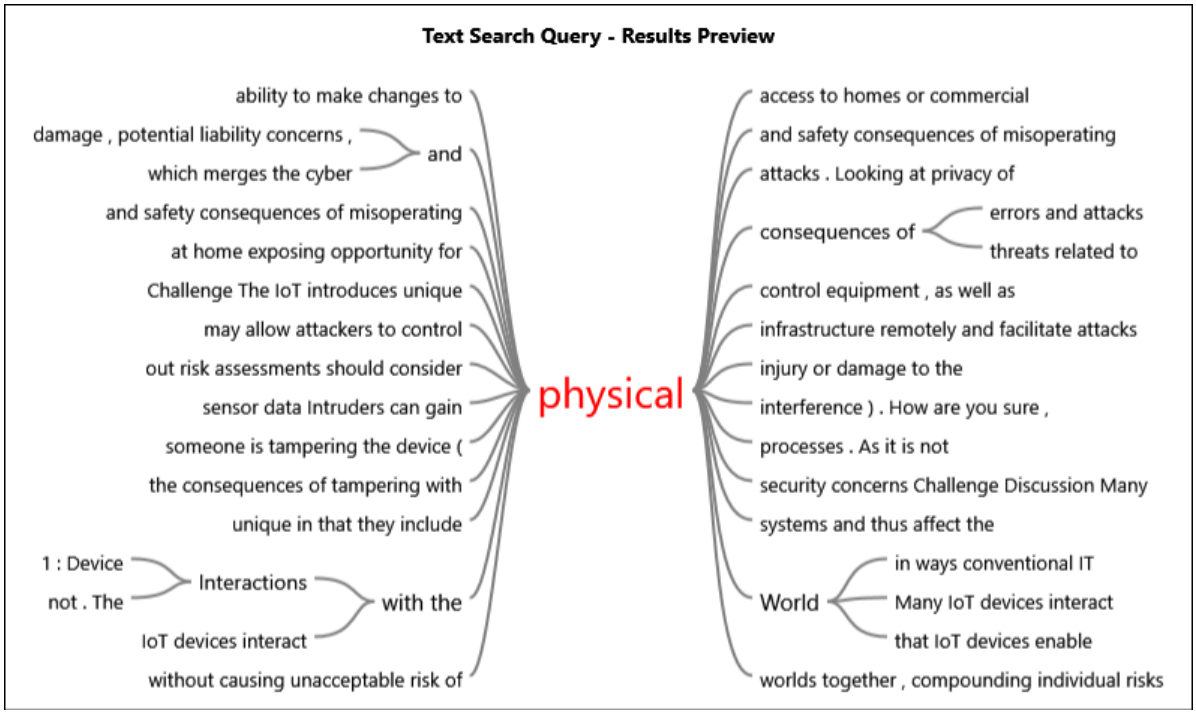


Figure C12: Word tree for 'physical' under the risk node

Figure C13: Word tree for 'availability' under the size and structure node

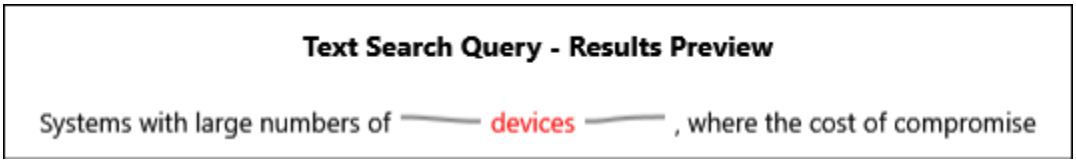


Figure C14: Word tree for 'devices under the size and structure node

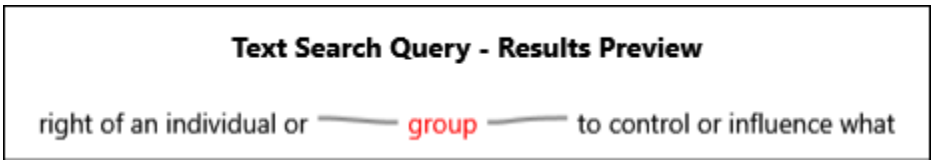


Figure C15: Word tree for 'group' under the size and structure node

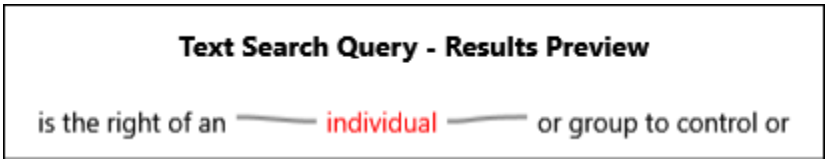


Figure C16: Word tree for 'individual' under the size and structure node

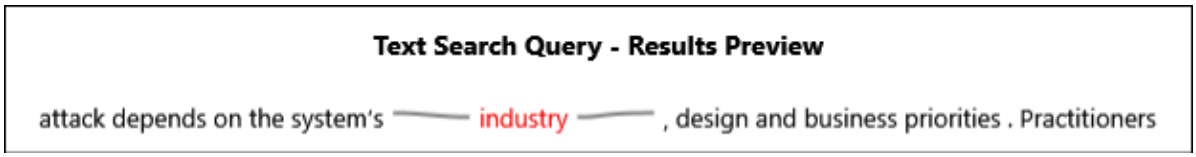


Figure C17: Word tree for 'industry' under the size and structure node

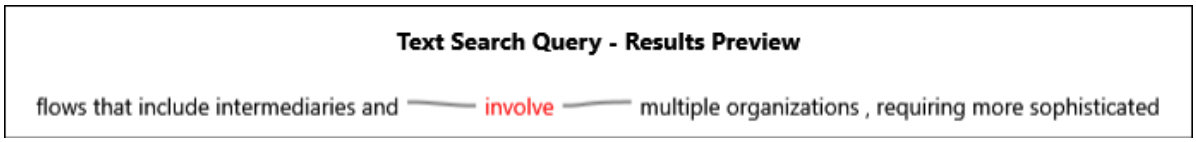


Figure C18: Word tree for 'involve' under the size and structure node

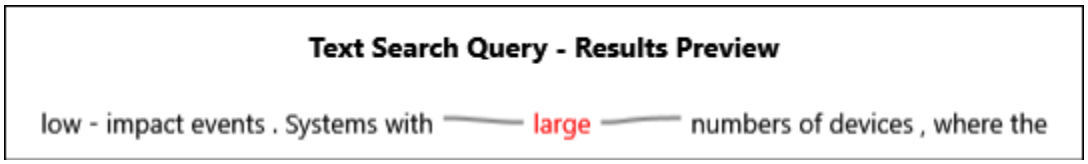


Figure C19: Word tree for 'large' under the size and structure node

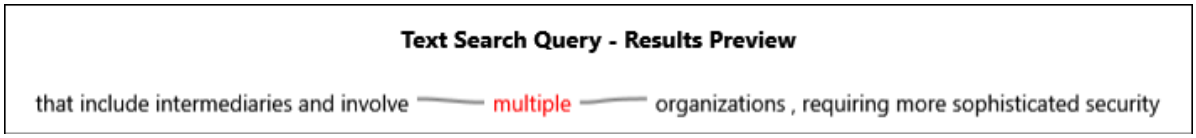


Figure C20: Word tree for 'multiple' under the size and structure node

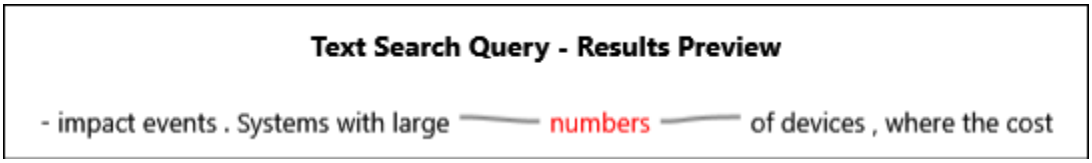


Figure C21: Word tree for 'numbers' under the size and structure node

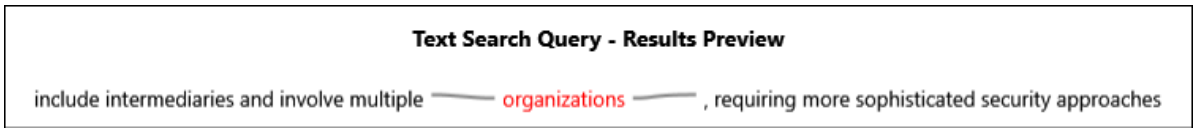


Figure C22: Word tree for 'organizations' under the size and structure node

Figure C23: Word tree for 'posture' under the size and structure node

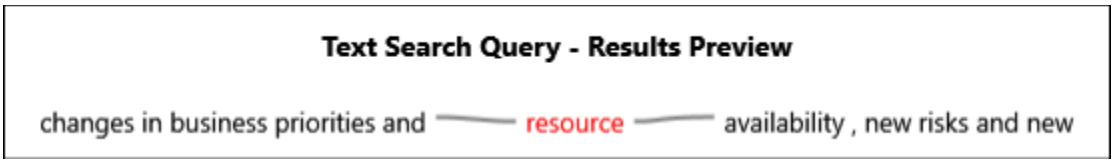


Figure C24: Word tree for 'resource' under the size and structure node

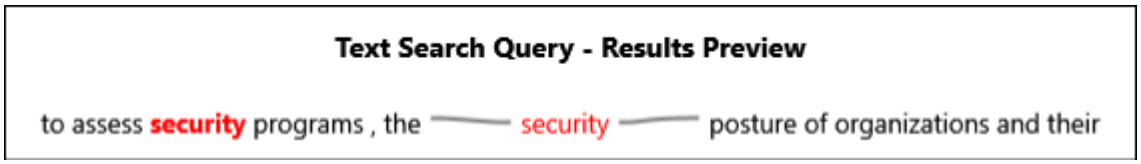
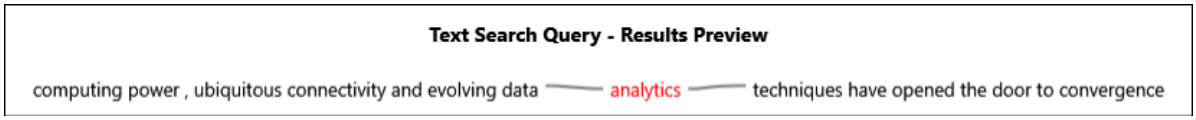


Figure C25: Word tree for 'security' under the size and structure node



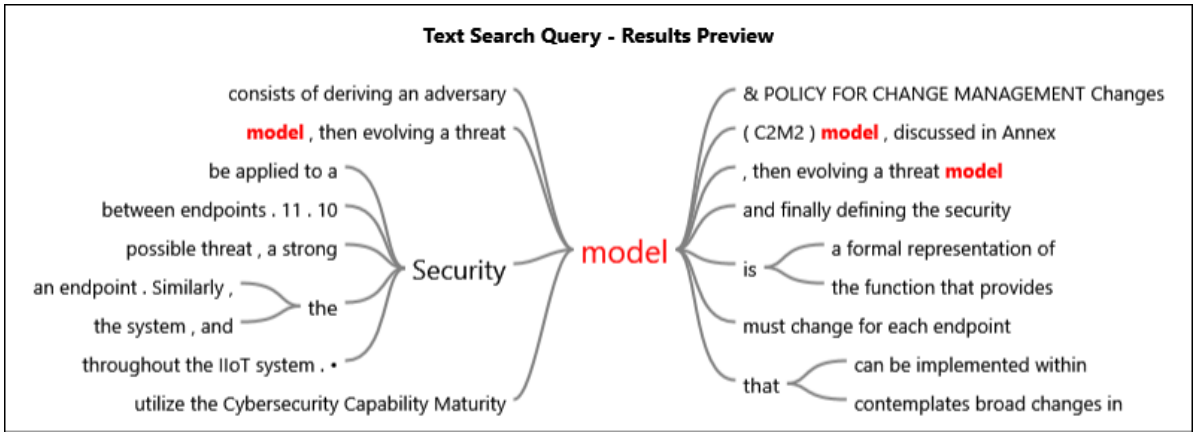


Figure C26: Word tree for 'model' under the cybersecurity structure node

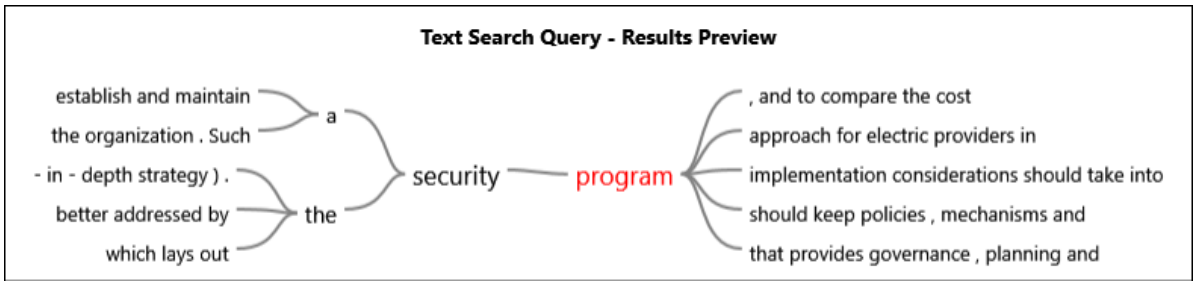


Figure C27: Word tree for 'program' under the cybersecurity structure node

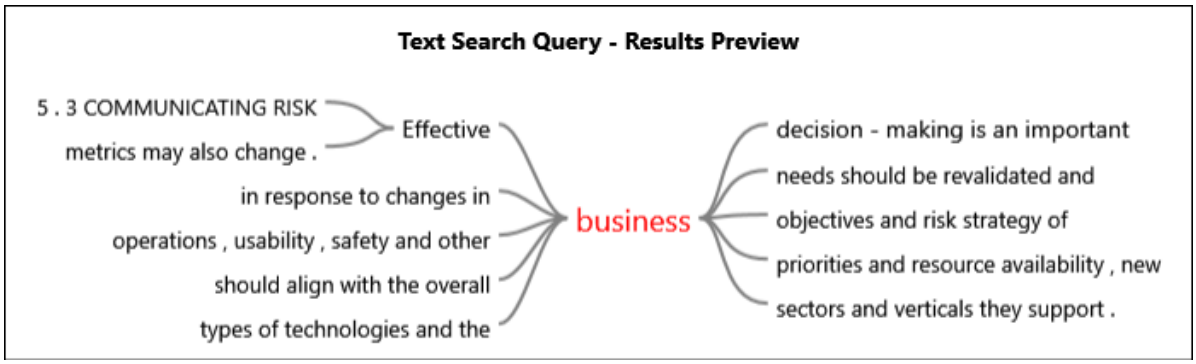


Figure C28: Word tree for 'business' under the cybersecurity structure node

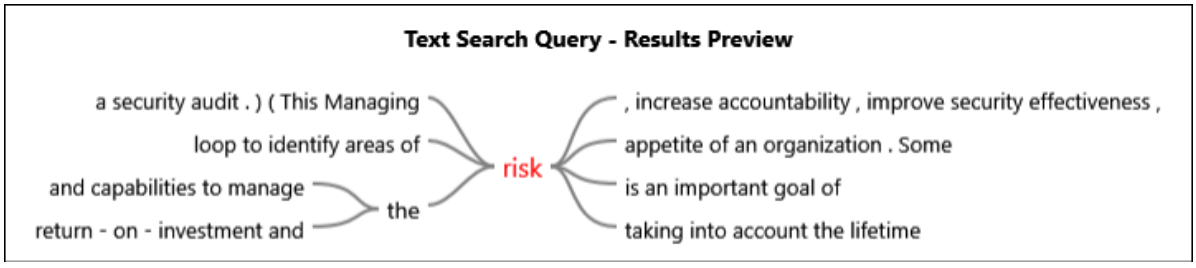


Figure C29: Word tree for 'risk' under the cybersecurity structure node

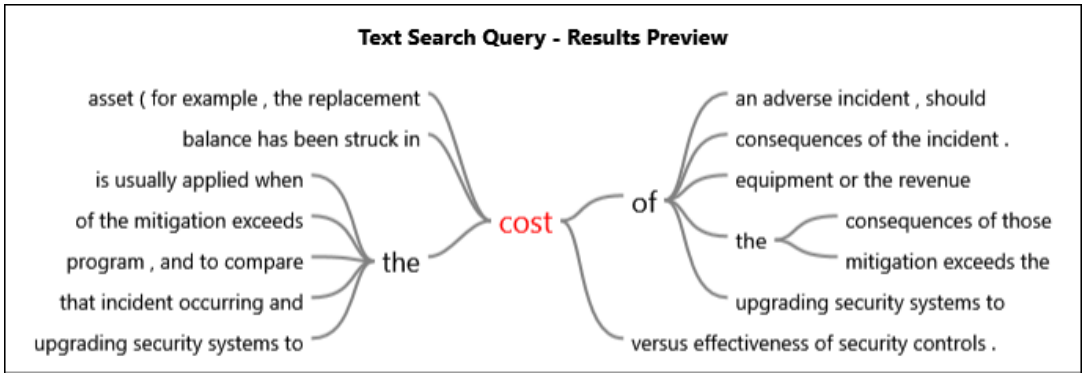


Figure C30: Word tree for 'cost' under the risk appetite node

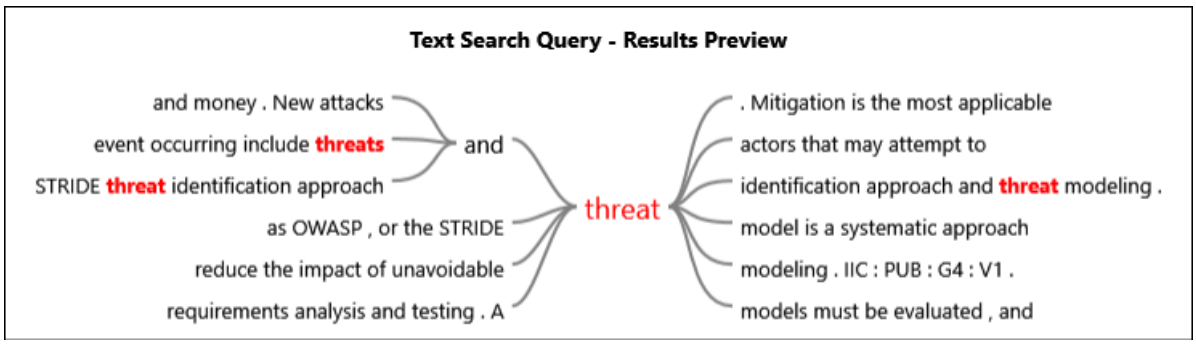


Figure C31: Word tree for 'threat' under the risk appetite node

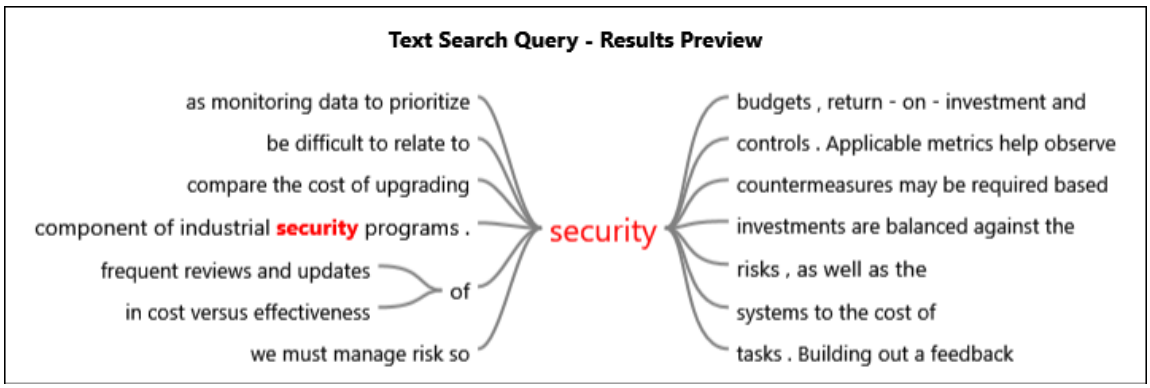


Figure C32: Word tree for 'security' under the risk appetite node

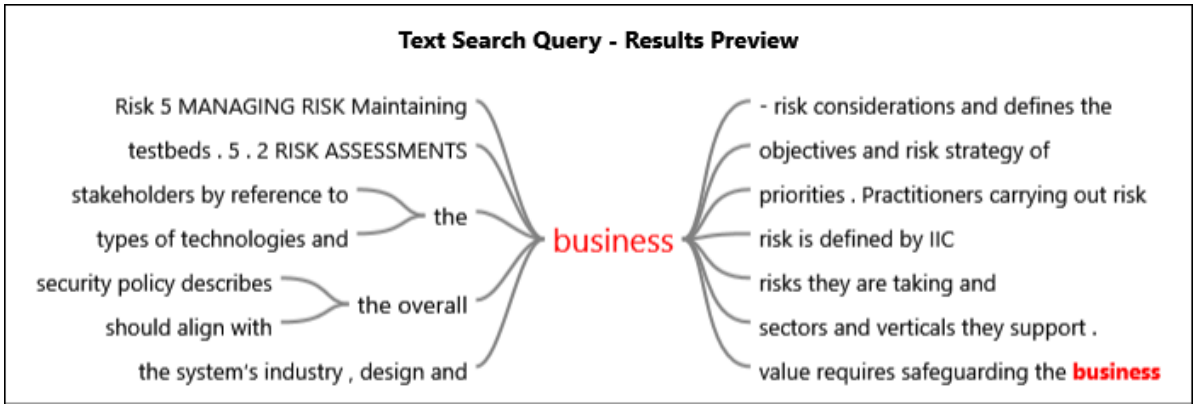


Figure C33: Word tree for 'business' under the risk appetite node

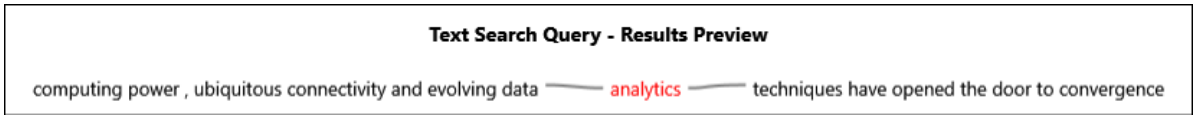


Figure C34: Word tree for 'analytics' under the innovativeness culture node

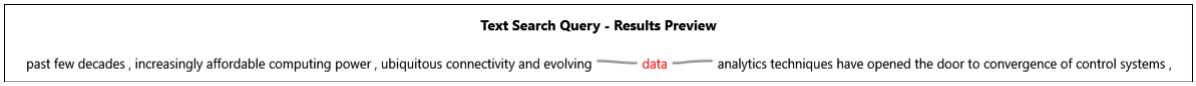


Figure C35: Word tree for 'data' under the innovativeness culture node

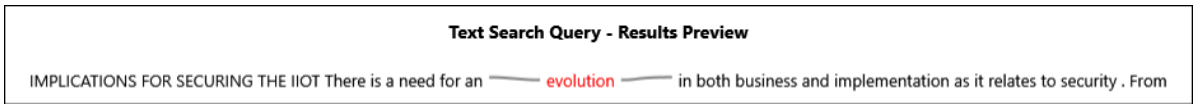


Figure C36: Word tree for 'evolution' under the innovativeness culture node

Figure C37: Word tree for 'expertise' under the innovativeness culture node

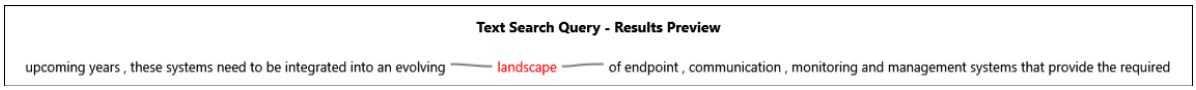


Figure C38: Word tree for 'landscape' under the innovativeness culture node

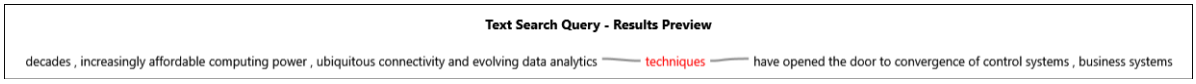


Figure C39: Word tree for 'techniques' under the innovativeness culture node

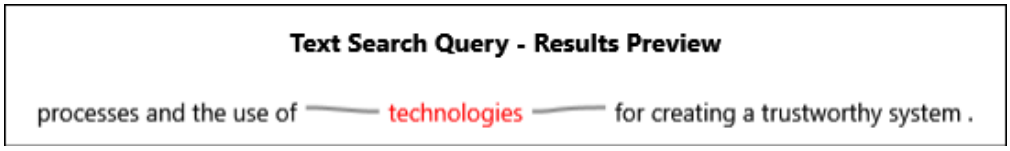


Figure C40: Word tree for 'technologies' under the innovativeness culture node

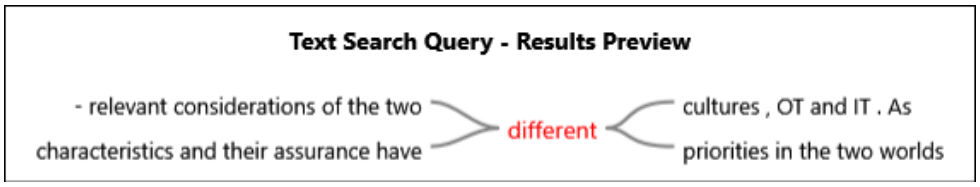


Figure C41: Word tree for 'different' under the security culture node

Figure C42: Word tree for 'convergence' under the security culture node

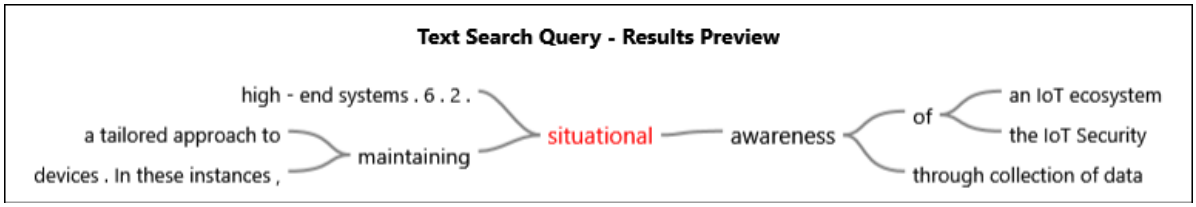


Figure C43: Word tree for 'situational' under the security culture node

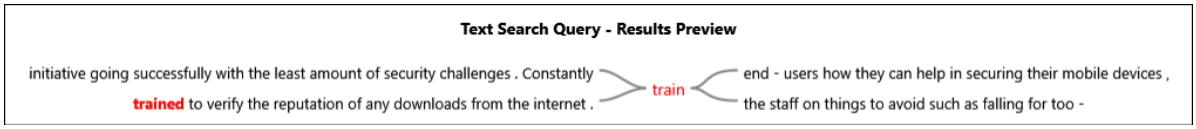


Figure C44: Word tree for 'train' under the security culture node

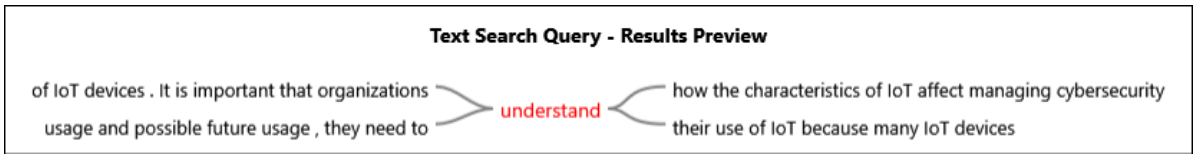


Figure C45: Word tree for 'understand' under the security culture node

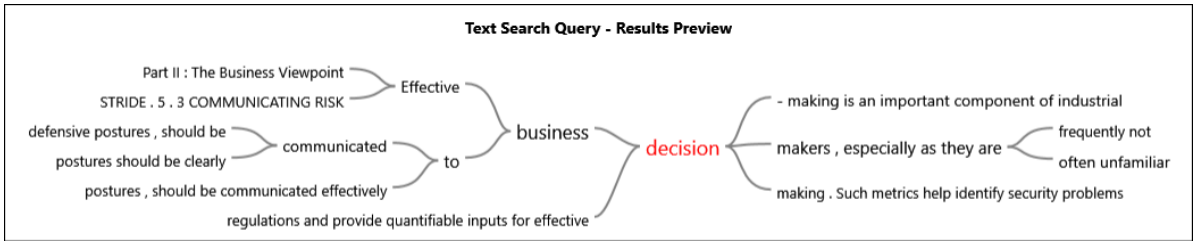


Figure C46: Word tree for 'decision' under the senior executive engagement node

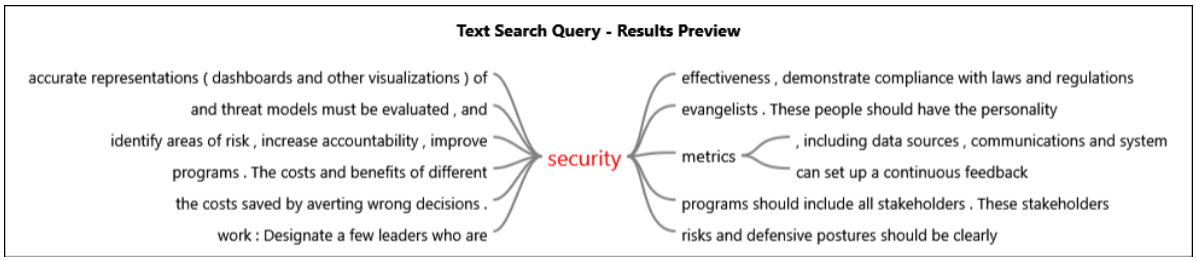


Figure C47: Word tree for 'security' under the senior executive engagement node

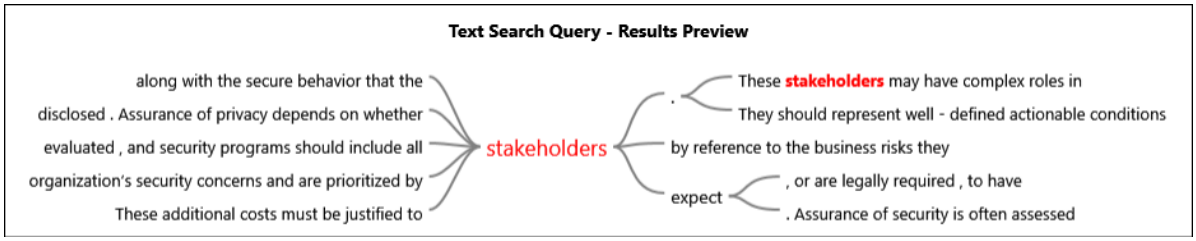


Figure C48: Word tree for 'stakeholders' under the senior executive engagement node

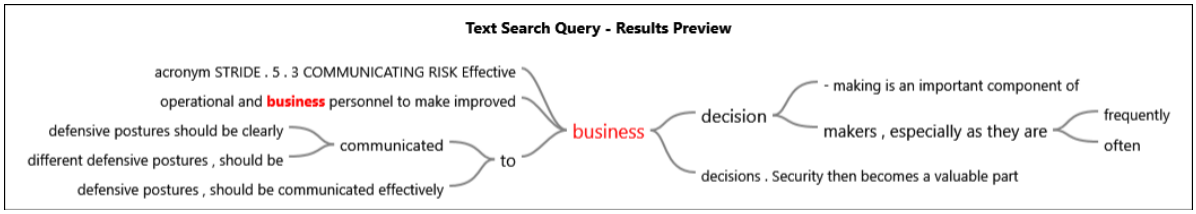


Figure C49: Word tree for 'business' under the senior executive engagement node

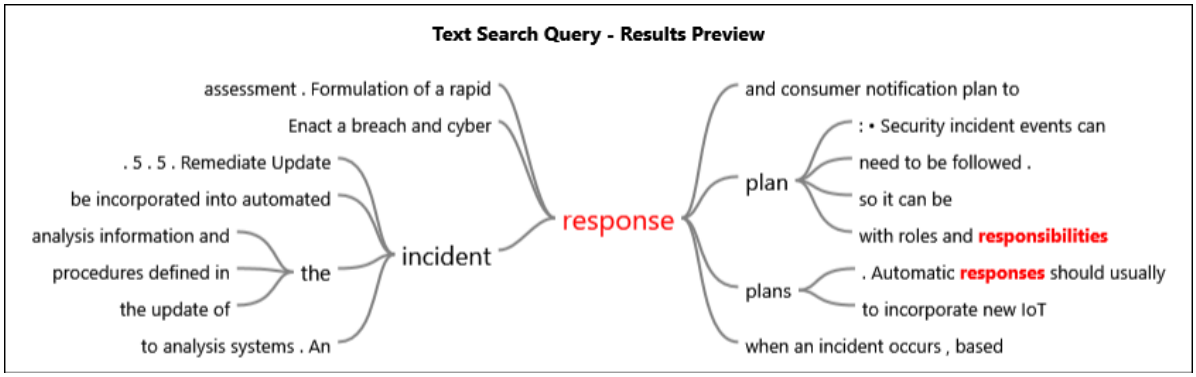


Figure C50: Word tree for 'response' under security incident response node

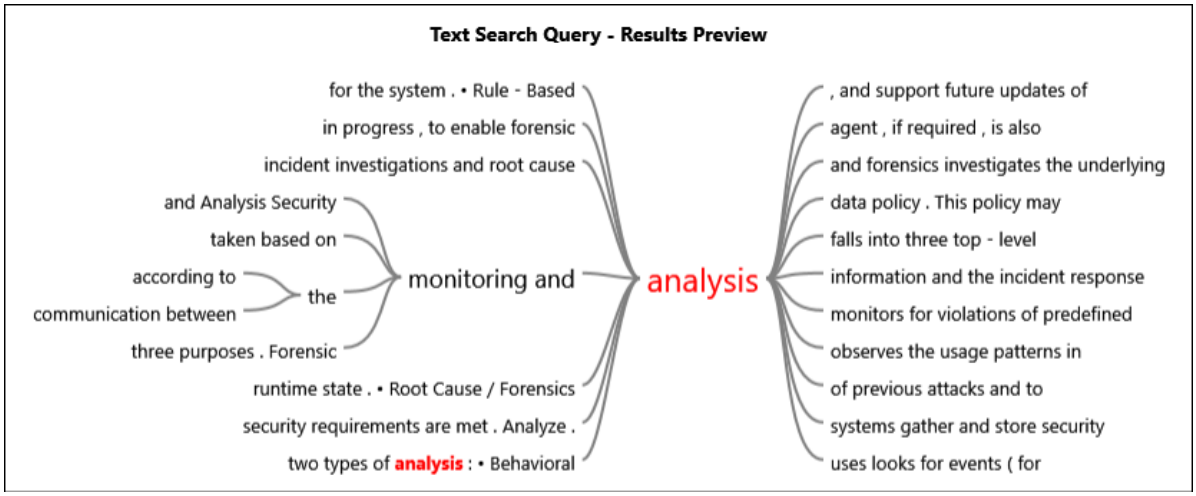


Figure C51: Word tree for 'analysis' under security incident response node

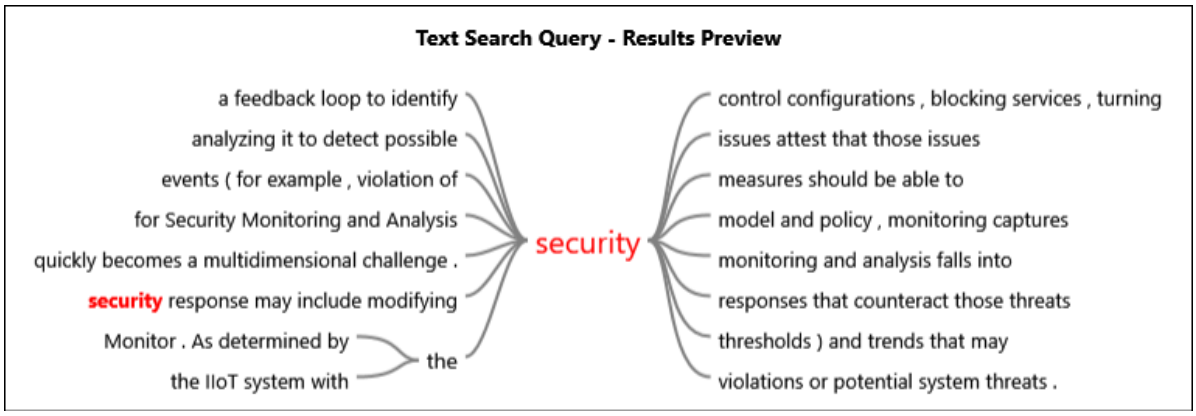


Figure C52: Word tree for 'security' under security incident response node

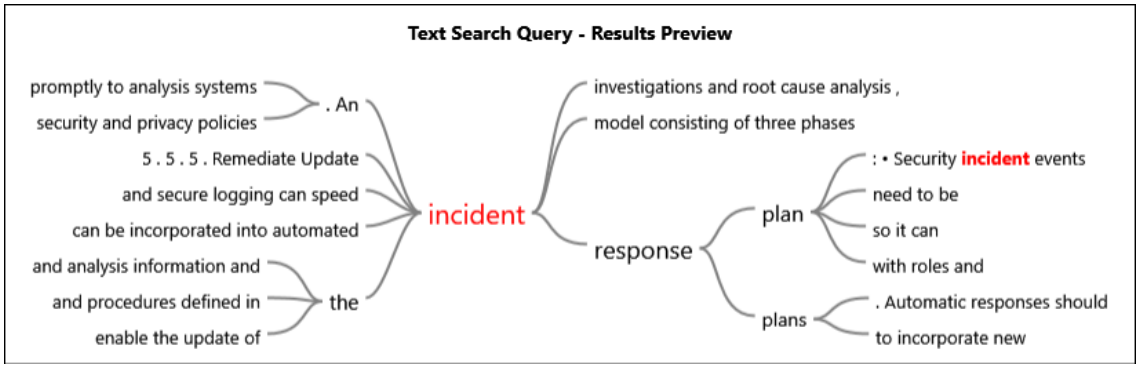


Figure C53: Word tree for 'incident' under security incident response node

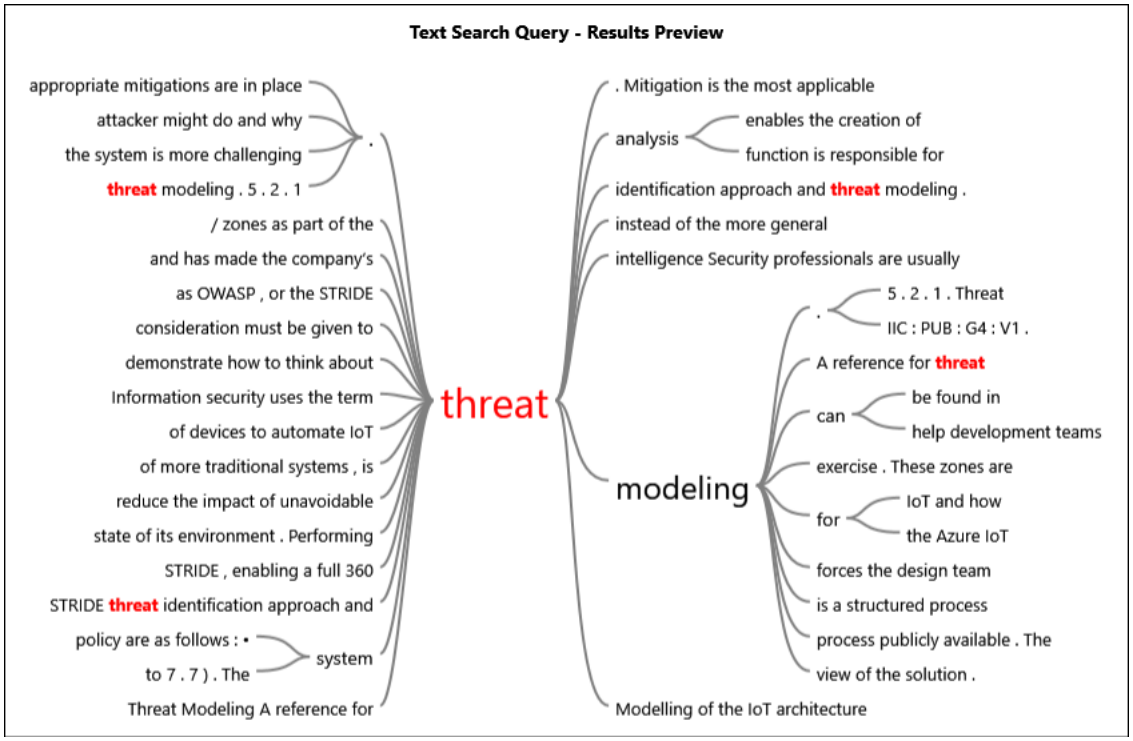


Figure C54: Word tree for 'threat' under risk management node

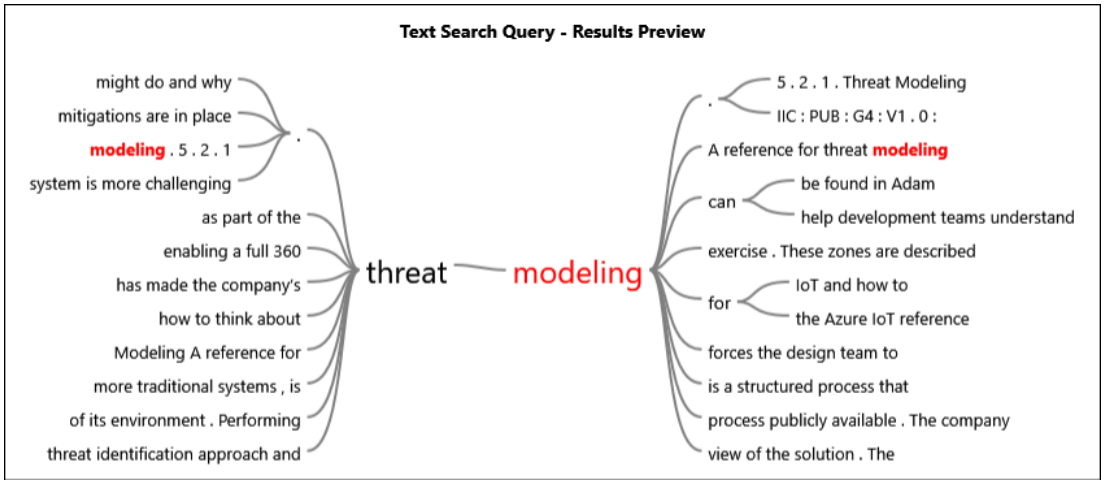


Figure C55: Word tree for 'modelling' under risk management node

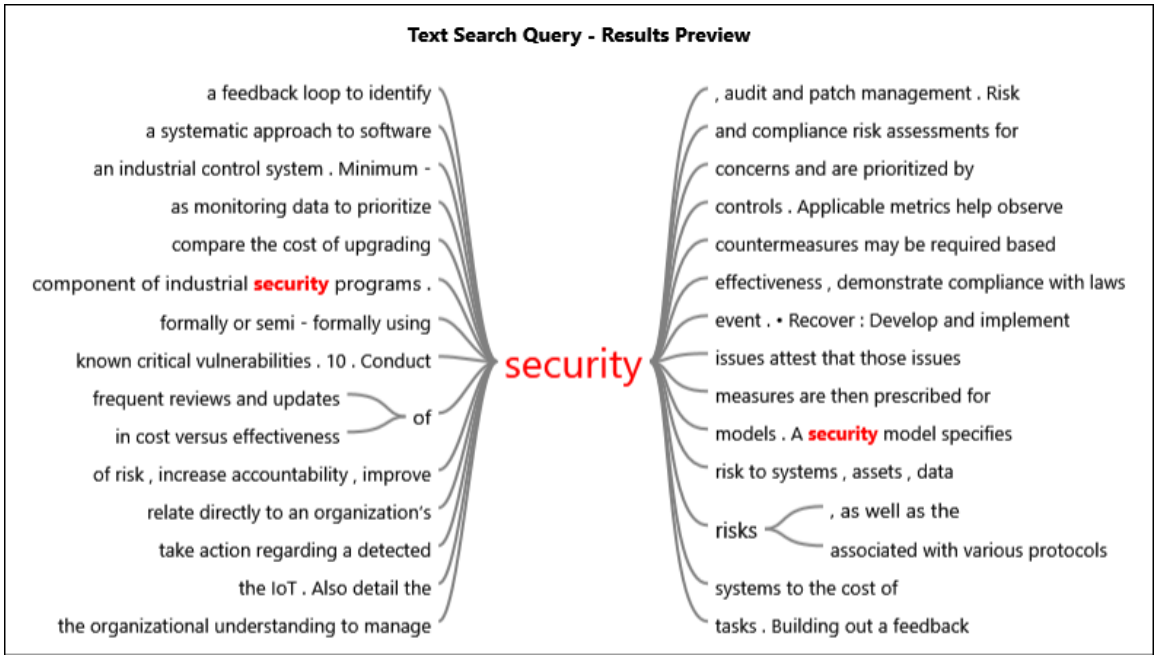


Figure C56: Word tree for 'security' under risk management node

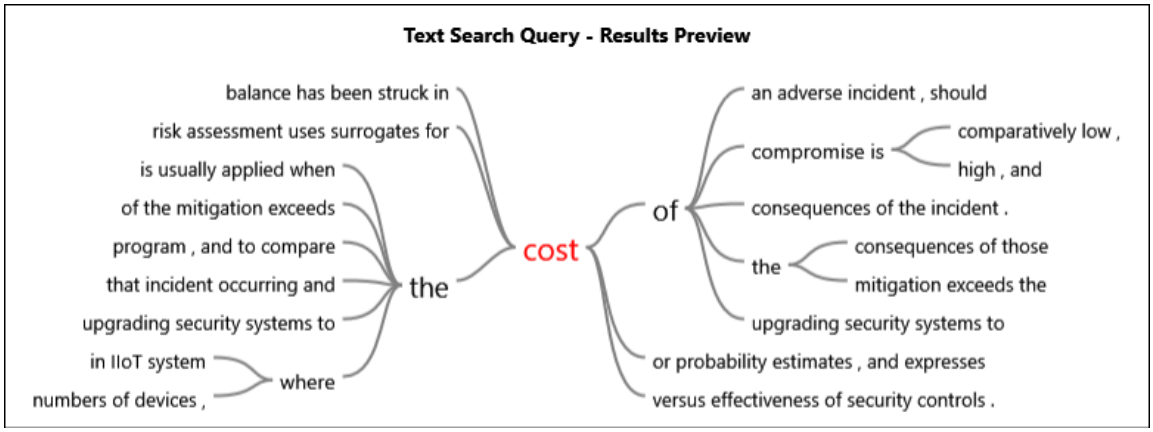


Figure C57: Word tree for 'cost' under risk management node

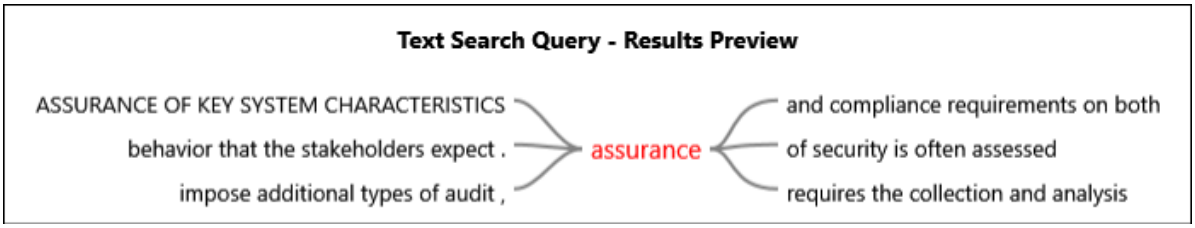


Figure C58: Word tree for 'assurance' under IT governance and compliance node

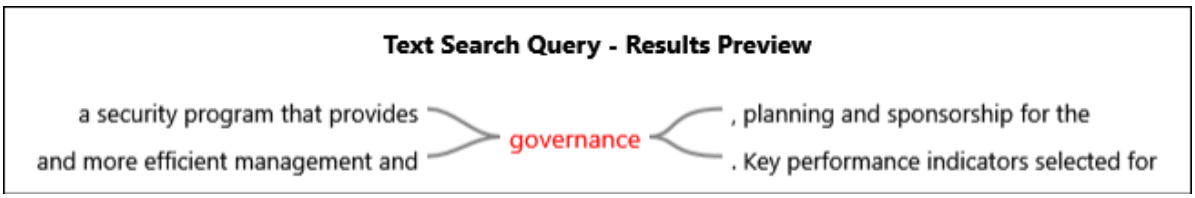


Figure C59: Word tree for 'governance' under IT governance and compliance node

Figure C60: Word tree for 'management' under IT governance and compliance node

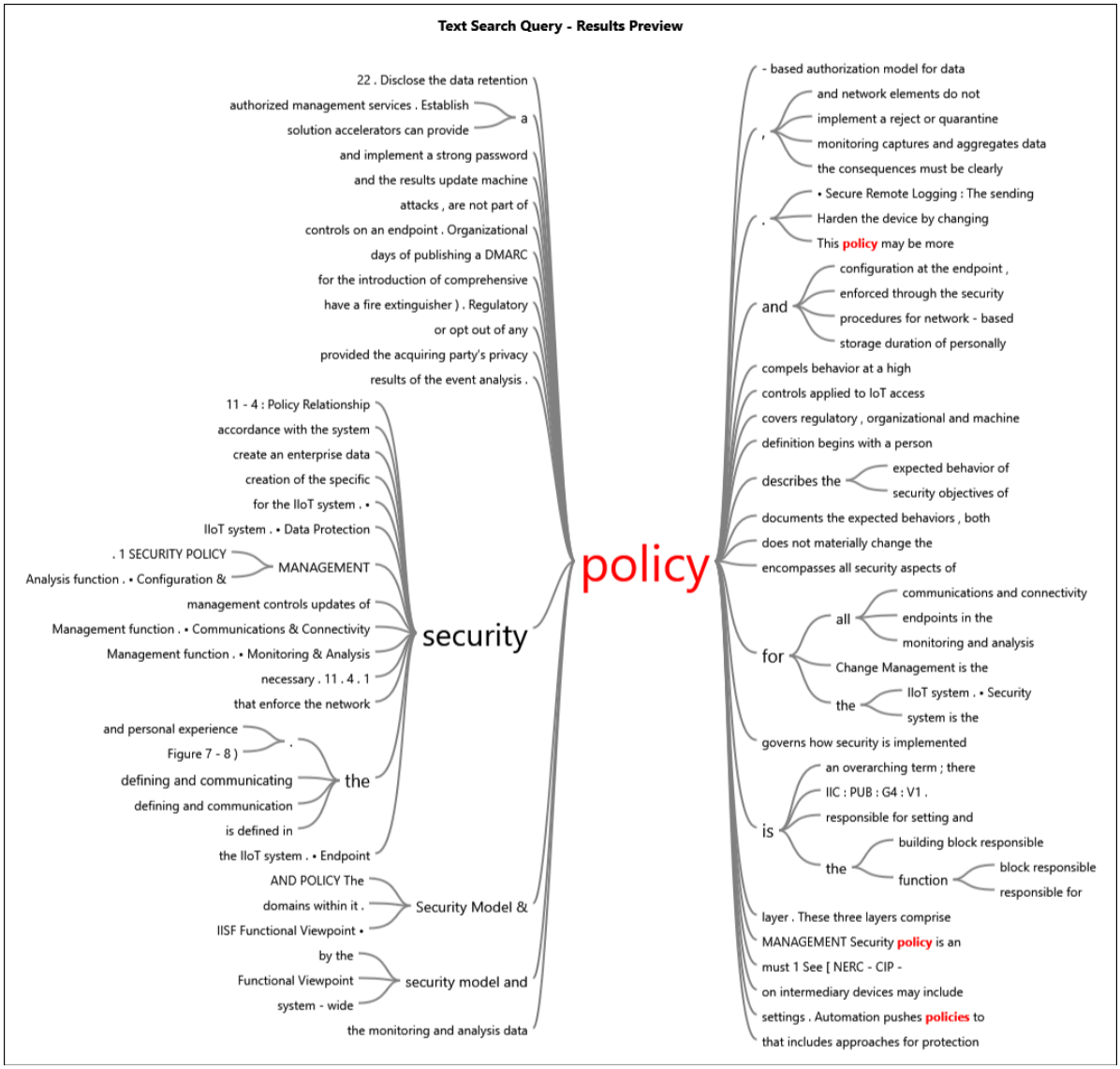


Figure C61: Word tree for 'policy' under policies, standards, and procedures node

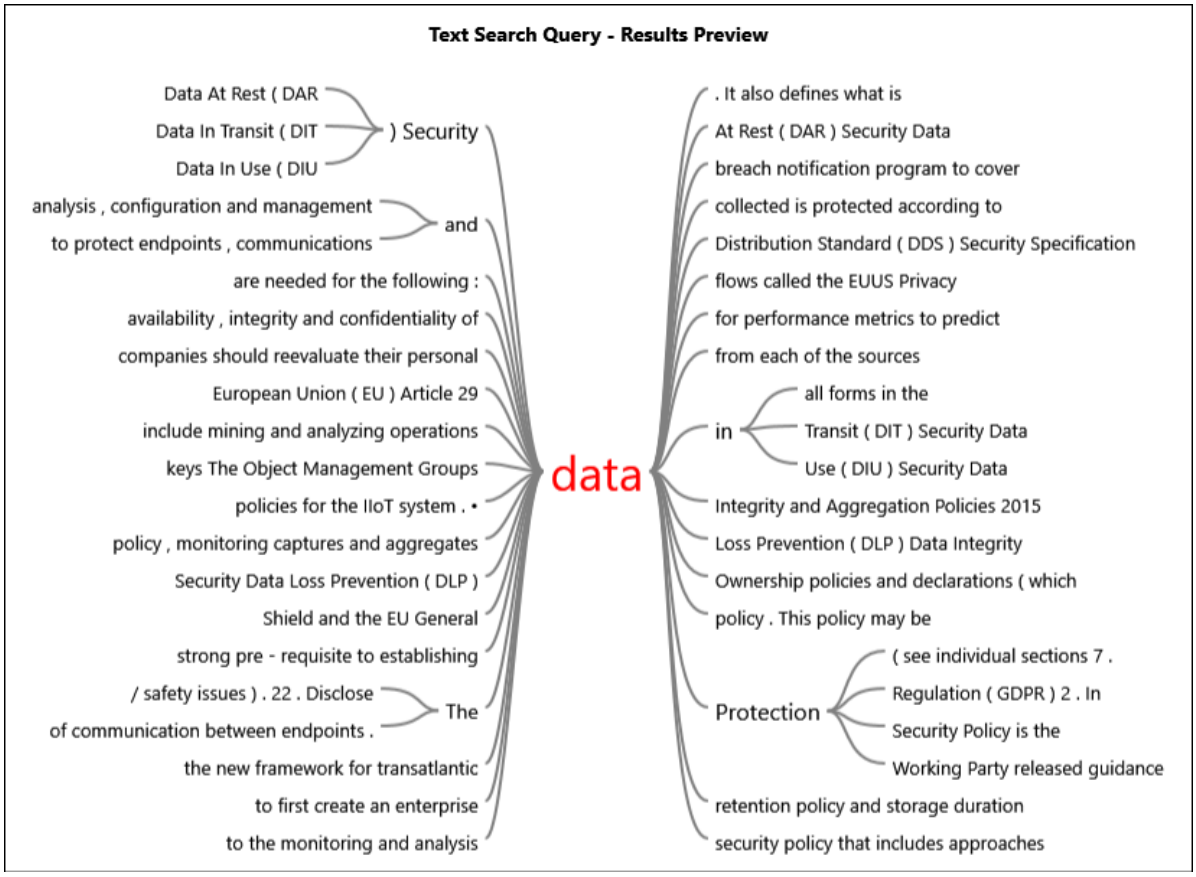


Figure C62: Word tree for 'data' under policies, standards, and procedures node

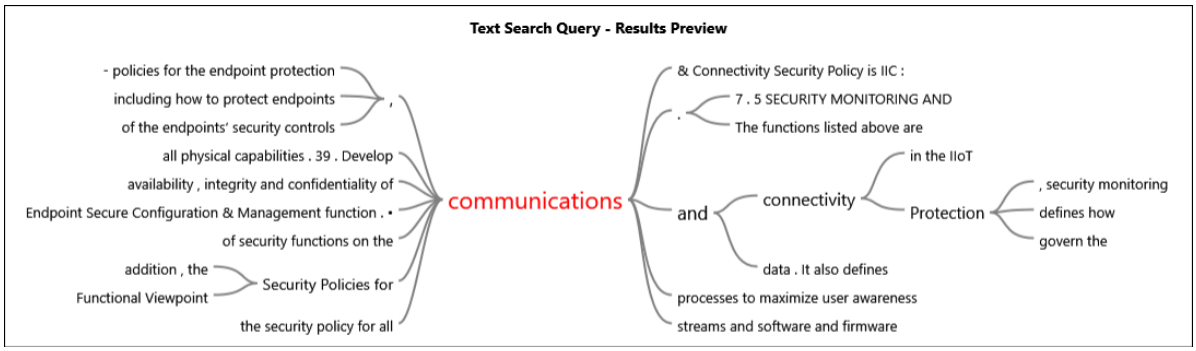


Figure C63: Word tree for 'communications' under policies, standards, and procedures node

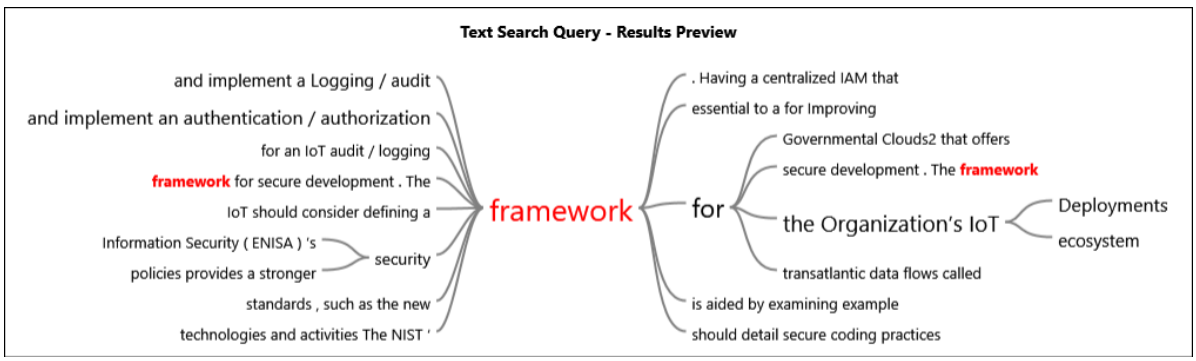


Figure C64: Word tree for 'framework' under policies, standards, and procedures node

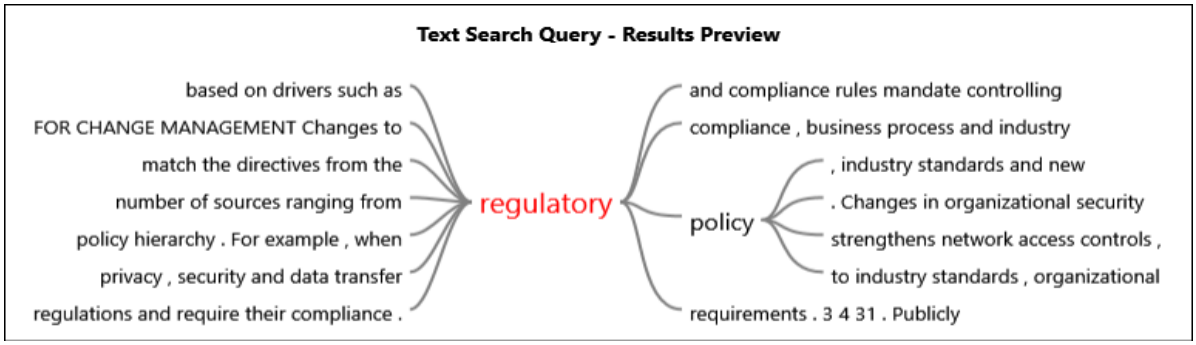


Figure C65: Word tree for 'regulatory' under legal and regulatory requirements node

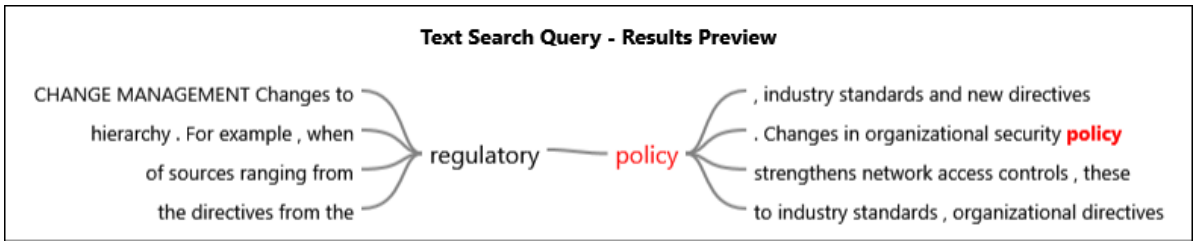


Figure C66: Word tree for 'policy' under legal and regulatory requirements node

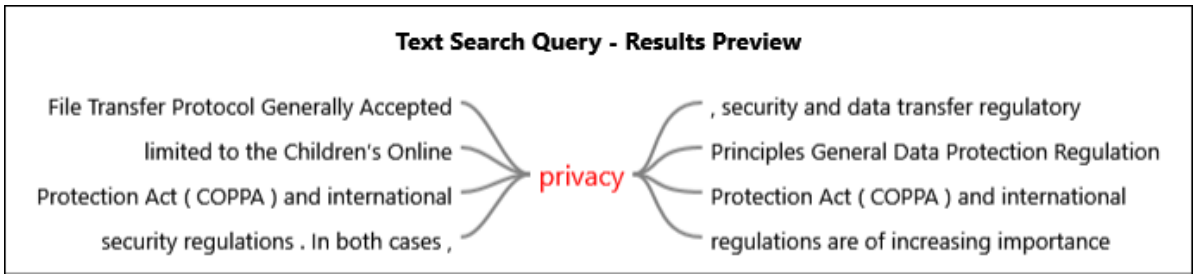


Figure C67: Word tree for 'privacy' under legal and regulatory requirements node

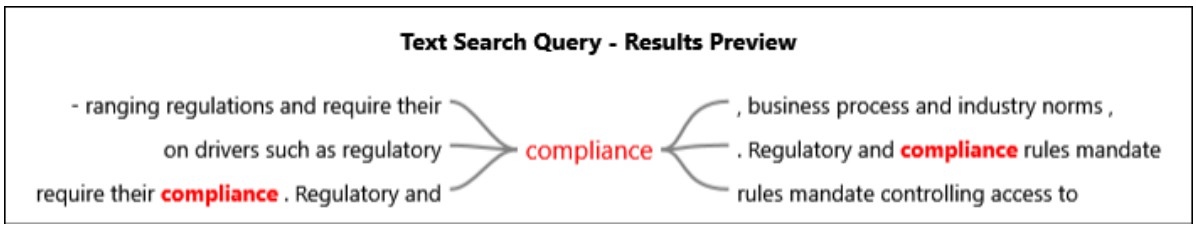


Figure C68: Word tree for 'compliance' under legal and regulatory requirements node

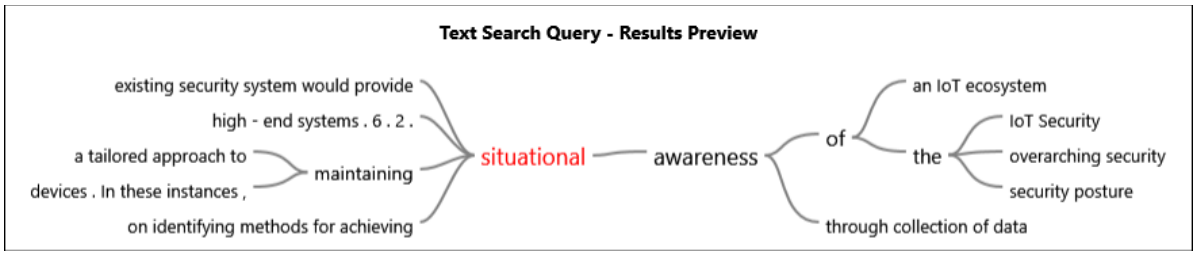


Figure C69: Word tree for 'situational' under cybersecurity awareness node

.

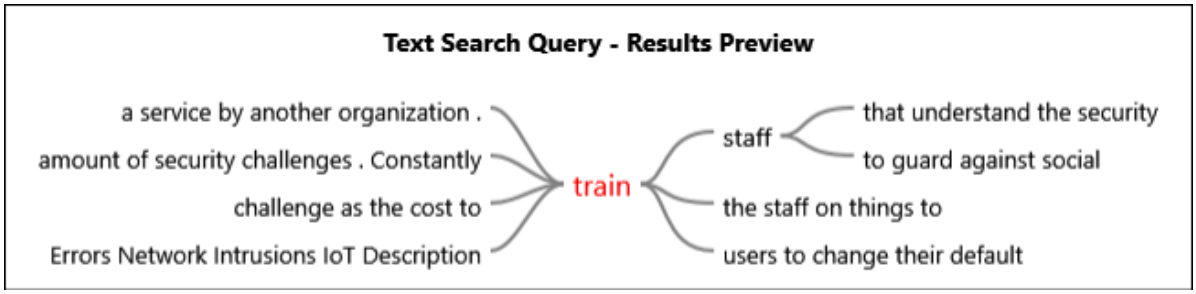


Figure C70: Word tree for 'train' under cybersecurity awareness node

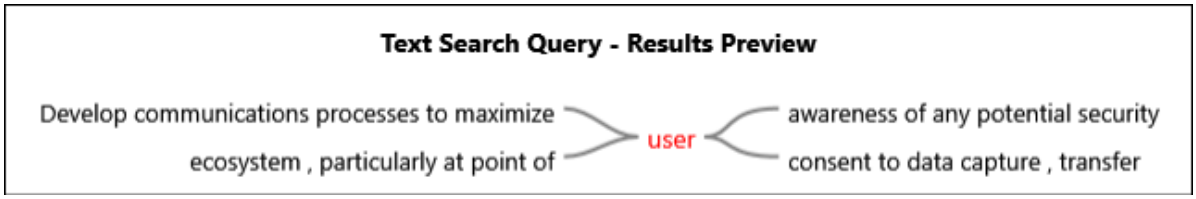


Figure C71: Word tree for 'user' under cybersecurity awareness node

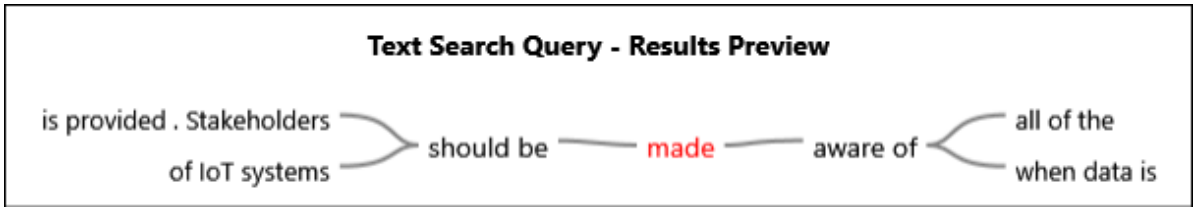


Figure C72: Word tree for 'made' under cybersecurity awareness node

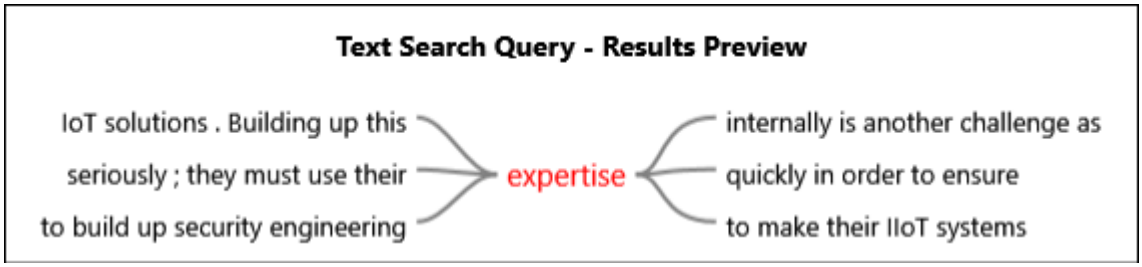


Figure C73: Word tree for 'expertise' under enablement node

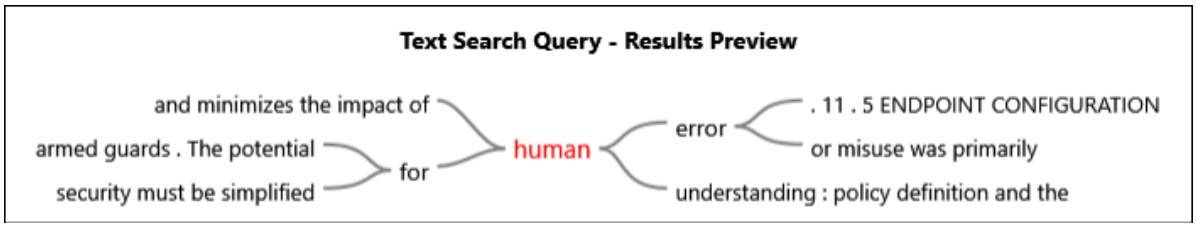


Figure C74: Word tree for 'human' under enablement node

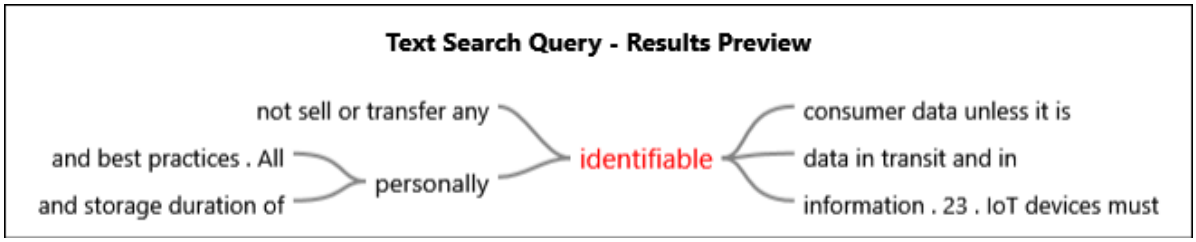


Figure C75: Word tree for 'identifiable' under enablement node

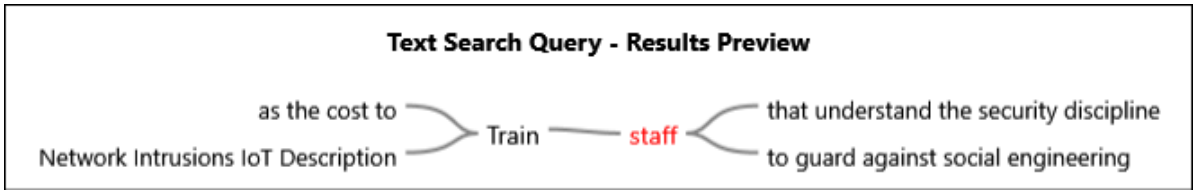


Figure C76: Word tree for 'staff' under enablement node

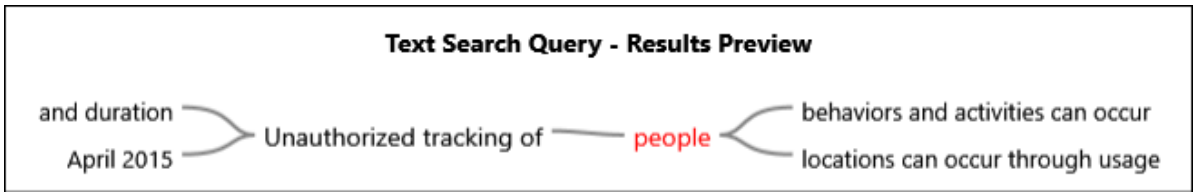


Figure C77: Word tree for 'people' under employee engagement node

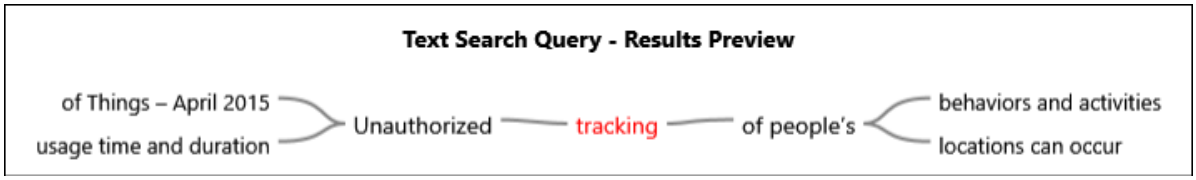


Figure C78: Word tree for 'tracking' under employee engagement node

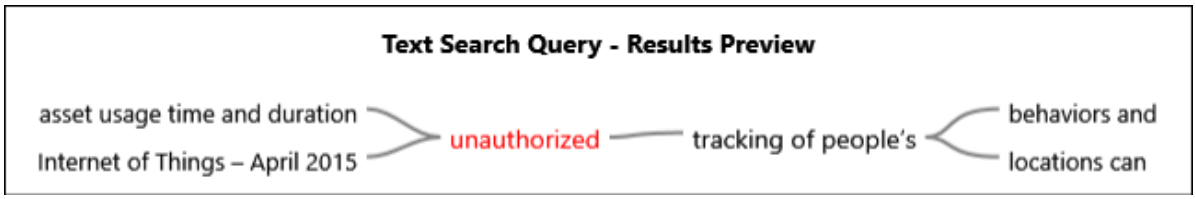


Figure C79: Word tree for 'unauthorised' under employee engagement node

Figure C80: Word tree for 'reward' under employee satisfaction node

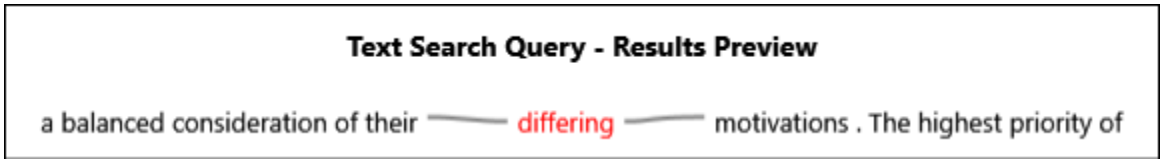


Figure C81: Word tree for 'differing' under employee satisfaction node

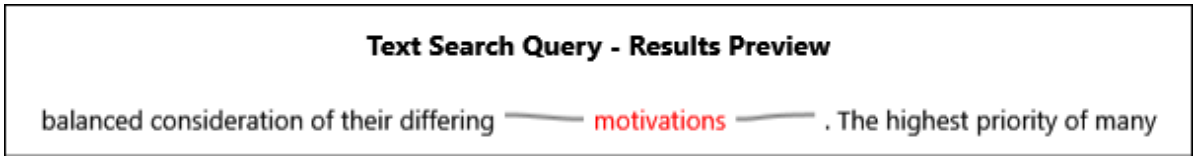


Figure C82: Word tree for 'motivations' under employee satisfaction node

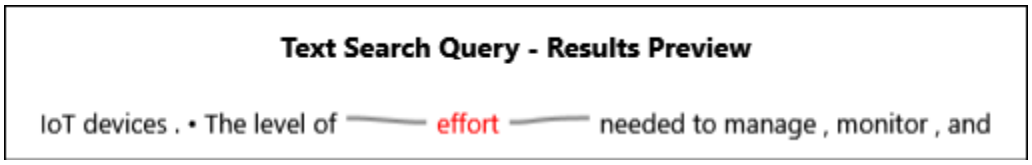


Figure C83: Word tree for 'effort' under employee satisfaction node

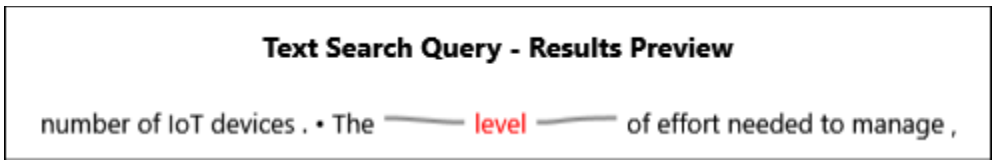


Figure C84: Word tree for 'level' under employee satisfaction node

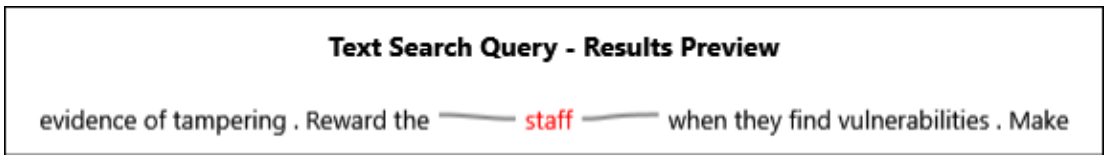


Figure C85: Word tree for 'staff' under employee satisfaction node

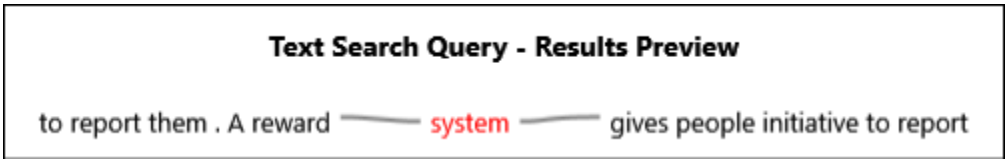


Figure C86: Word tree for 'system' under employee satisfaction node

Appendix D Shodan Results

Table D1: List of IIoT device exposed to the Internet

Source: Author Compiled

Protocol	Description	No of IIoT devices in South Africa exposed to the internet
MQQT (Message Queuing Telemetry Transport)	The MQTT Is an IIoT message protocol developed in 1999. It is commonly used for remote monitoring in IIoT applications, particularly for gathering data from numerous electrical devices. The MQTT protocol operates on a hub-and-spoke architecture and relies on TCP for reliable data transmission. It consists of three key components: Subscriber, Publisher, and Broker. The Publisher generates and sends data; the Broker facilitates the communication between Publishers and Subscribers, and the Subscriber receives the data. The Broker also ensures security by verifying the authorisation of Subscribers and Publishers (Hasan, 2023).	889
AMQP (Advanced Message Queuing Protocol)	AMQP is a widely adopted open standard that facilitates the exchange of business messages between applications or organisations. It establishes connections between systems, delivers essential information to support business processes, and ensures the reliable transmission of instructions to accomplish their objectives (Tezer, 2013).	412
CoAP (Constrained Application Protocol)	CoAP is designed specifically for resource-constrained smart devices. It is intended to be used within networks of similar constrained devices, including general internet nodes and devices on restricted networks. It is suitable for IIoT systems that rely on HTTP protocols. It leverages the lightweight UDP protocol for efficient data transmission. CoAP adopts a RESTful architecture for ease of use and compatibility (Hasan, 2023).	28
DDS (Data-Distribution Service for Real-Time Systems)	DDS is a standardised protocol that enables high-performance, scalable, real-time communication between machines. DDS allows for data transfer in resource-constrained devices and cloud platforms and consists of two main layers: DCPS (Data-Centric Publish-Subscribe) and DLRL (Data-Local Reconstruction Layer). DCPS facilitates information delivery to subscribers, while DLRL provides an interface for accessing the functionalities of the Data-Centric Publish-Subscribe mechanism (Hasan, 2023).	10
TOTAL		**1,339**

Appendix E Ethical Clearance

UNIVERSITY OF
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

17 September 2019

Mr Barend Hendrik Pretorius (200276341)
School Of Man Info Tech & Gov
Westville Campus

Dear Mr Pretorius,

Protocol reference number: HSSREC/00000392/2019
Project title: Cybersecurity for Industrial Internet of Things: a case study of the South African transport sector

Full Approval – Expedited Application

This letter serves to notify you that your application received on 16 August 2019 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

This approval is valid for one year from 17 September 2019.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be sub[redacted]dy is finished.

Yours sincerely,

[redacted]

Dr Rosemary Sib[redacted]

/spm