An analysis of cybersecurity culture in an organisation managing Critical Infrastructure

By

Abraham Parbhunath

Supervisor:

Professor Thomas Meyer

Co-supervisor: Associate Professor Louise Leenen

Dissertation presented in partial fulfilment of the requirements

for the degree of

Master of Science

Department of Computer Science

Faculty of Science

University of Cape Town

January 2021

Dedicated to

My Family (Olivia, Tashiana and Ashriya)

Abstract

The 4th industrial revolution (4IR) is transforming the way businesses operate, making them more efficient and data-driven while also increasing the threat-landscape brought on by the convergence of technologies and increasingly so for organisations managing critical infrastructure. Environments that traditionally operated entirely independent of networks and the internet are now connecting in ways that are exposing critical infrastructure to a new level of cyber-risks that now need to be managed. Due to the stable nature of technologies and knowledge in traditional industrial environments, there is a misalignment of skills to emerging technology trends. Globally cyber-crime attacks are on the rise with Cisco reporting in 2018 that 31% of all respondents had seen a cyber-attack in their operational environment[1]. With up to 67% of breaches reported in the Willis Towers report due to employee negligence [2], the importance of cybersecurity culture is no longer in question in organisations managing critical infrastructure. Developing an understanding of the drivers for behaviours, attitudes and beliefs related to cybersecurity and aligning these to an organisations risk appetite and tolerance is crucial to managing cyber-risk.

There is a very divergent understanding of cyber-risk in the engineering environment. This study endeavours to investigate employee perceptions, attitudes and values associated with cybersecurity and how these potentially affects their behaviour and ultimately the risk to the plant or organisation. Most traditional culture questionnaires focus on information security with observations focussing more on social engineering, email hygiene and physical controls. This cybersecurity culture study was conducted to gain insight into people's beliefs, attitudes and behaviours related to cybersecurity encompassing people, process and technology focussing on the operational technology environment in Eskom[1]. Both technical (Engineering and IT) and nontechnical (business support staff) staff were questionnaireed. The questionnaire was categorised into four sections dealing with cybersecurity culture as they relate to individuals, processes and technology, leadership and the organisation at large. The results from the analysis, revealed that collaboration, information sharing, reporting of vulnerabilities, high dependence and trust in technology, leadership commitment, vigilance, compliance, unclear processes and lack of understanding around cybersecurity all contribute to the current levels of cybersecurity culture. Insights from this study will generate recommendations that will form part of a cybersecurity culture transformation journey.

[1] Eskom is the electricity utility in South Africa https://www.eskom.co.za/Pages/Landing.aspx

Declaration

The work in this dissertation is based on the research carried out in the department of computer science at the University of Cape Town as part of the completion of my Master's degree. I declare that no part of this work has been submitted elsewhere for any purpose. I declare that these are my own words except where references are given of texts or diagrams. I declare that I have submitted an original work written in my own words. With the signature, I declare that I have been informed about normal academic citation rules and I conform to citation convention customary to the sciences. This written work may be tested electronically for plagiarism.

Signed by candidate

Signature: Abraham Parbhunath Date: February 2021

Acknowledgement

I am indebted to Eskom Nuclear Engineering for providing financial assistance that enabled me to carry out this research. I am grateful to my supervisors, Professor Tommie Meyer and Professor Louise Leenen, for their guidance, understanding and encouragement throughout the process of completing this dissertation. A special thanks to Professor Tommie who stuck with his commitment to supervise me even though he was on sabbatical.

I am thankful to Security Solutions (Cyber) CoE without whose support the study would have been extremely difficult to carry out, as well as the various departments like Enterprise Risk and Sustainability and governance committees that challenged and championed this initiative.

I am forever grateful to my family, especially my wife; Olivia and kids Tashiana and Ashriya, for all the support, encouragement and understanding I received from them during my studies. I learnt a valuable lesson that nothing worth doing is ever easy and hopefully this will inspire them one day to also be tenacious in the quest for understanding and self-development. COVID19 threw us a major curve ball, but through it all, we pushed through, survived and made a success of it- testimony of the indomitable human spirit!

Table of Contents

List of Tables

List of Figures

Abbreviations

BMIS	Business Model for Information Security
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CMM	Capability Maturity Model
CNC	Computer Numerical Control
COBIT	Control Objectives for Information Technology
CPD	Continuous Professional Development
DCS	Distributed Control System
DDOS	Distributed Denial of Service
DLP	Data Loss Prevention
DMZ	Demilitarised Zone
ECSA	Engineering Council of South Africa
ENISA	European Union Agency for Cybersecurity
GIT	Group IT
GRC	Governance Risk Compliance
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPS	Intrusion Protection system
ISACA	Information Systems Audit and Control Association
ISC	Information Security Culture
ISO	International Organisation for Standardisation
IoT	Internet of Things
IIoT	Industrial Internet of Things
IRM	Integrated Risk Management

IT	Information Technology
ITU	International Telecommunication Union
NCII	National Critical Information Infrastructure
NCPF	National Cybersecurity Policy Framework
NIST	National Institute of Science and Technology
OT	Operational Technology
OTS	Off-the Shelf
PDCA	Plan-Do-Check-Act
PLC	Programmable Logic Controller
PMT	Protection Motivation Theory
PWC	Price- Waterhouse-Coopers
RTU	Remote terminal unit
SCADA	Supervisory Control and Data Acquisition
SCOT	Steering Committee of Technology
SSA	State Security Agency
SSC (CoE)	Security Solutions (Cyber): Centre of Excellence
TPB	Theory of Planned Behaviour
UTM	Unified Threat Management

1. Introduction

Eskom is a large organ of state that manages the generation, transmission and distribution of electricity for South Africa. The production and sale of electricity is regulated by the South African government via the National Electricity Regulator of South Africa (NERSA) [2] with strict operating guidelines for this industry as well as tariff structures that control pricing. The Critical Infrastructure Protection Act 8 of 2019 defines critical infrastructure as any building, centre, establishment, facility, installation, pipeline, premises of systems needed for the functioning of society, the government or enterprises of the Republic and includes networks for the delivery of electricity or water [3]. The supply of electricity has been declared an essential service and the infrastructure that enables this service has been declared to be critical infrastructure. The critical infrastructure comprises plant systems, network management, supervisory and control systems, protection systems all of which have associated industrial control and automation systems that manage their safe and reliable operations. In the past, these systems used proprietary protocols for communication that were non-routable and not internet facing, however due to technological advancements and increasing requirements for standardisation there is movement away from these and consequent convergence between Information Technology (IT) and Operational Technologies (OT). IT commonly refers to a large spectrum of technologies used for corporate information processing including software, hardware and related services and includes unified communications. OT refers to the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, actuators etc. such as the control system for a power station. The resulting threat landscape related to this convergence is no longer that of insider threats but has now evolved to a cyber-physical risk. Cyber-risks are controlled by having robust processes in place, implementation of technology that automatically detects and protects against attacks and having employees that are aware of cyber-risk and are suitably trained with appropriate behaviours and attitudes to minimise the human error that can initiate a cyber-attack.

Although cyber-attacks are predominantly digitally or technologically executed, human negligence or lack of judgement has very often been found to be the root cause of exploitation. A cyber-attack can have a localised impact or depending on how advanced the attack is, can bring a country to a standstill. Globally cyber-crime attacks are on the rise, with Cisco reporting in a questionnaire conducted in 2018 that 31% of all respondents had seen a cyber-attack in their operational environment and 90% believing that Operational Technology (OT) is at risk to cyber threats [1]. SecurityIntelligence.com reported 2788 attacks against industrial control systems (ICS) in 2017 with attacks increasing by over 2000% since 2018, and 2019 alone having more attacks on OT systems than the previous three years combined [4]. The OT security firm Claroty reported a 25% increase in the number of ICS vulnerabilities disclosed in 2020 from 2019, 70% of which could be exploited remotely [5]. It is evident that the number of cyber-attacks is growing at an unprecedented rate while the vulnerabilities are also increasing.

Eskom has over 44000 employees with a large number of them having access to both corporate and OT networks. The Willis Towers Consultancy report of 2017 highlighted that up to 67% of breaches captured was due to employee negligence [2]. Considering the large staff complement of Eskom, with various levels of knowledge on cybersecurity, the risk exposure due to staff interaction with technology is significant. Culture is an integral part of cybersecurity effectiveness as it impacts on those elements that have human influence in cyber-attacks [2].

[2] https://nersa.org.za/

Eskom is currently undergoing a restructure but is currently structured into three core divisions:

- Generation responsible for the generation of power using coal, nuclear, fossil, wind and hydro technologies;
- Transmission responsible for the transportation of power from the generation sites to the distribution sites;
- Distribution responsible for getting the power from the Transmission network to its customers who are either municipalities, businesses, industrial areas, or normal users.

The operation of the above divisions is enabled by a Telecoms Division that is responsible for the transport layer that supports both the IT and OT networks. The IT network is the corporate network that supports all support business processes like ERP (enterprise resource planning), finance, HR (human resources), commercial etc. and is managed by GIT (Group IT) who report to a CIO. The OT network is responsible for all the engineering and industrial control systems that support the core business of the production, transmission and distribution of electricity. Telecoms focus is end-to-end delivery with no interest in the actual traffic and its management for now and they have service level agreements (SLAs) with their customers. PTM&C (Protection, telecommunication, metering and control) is a very important part of OT network and the Telecoms division is responsible for ensuring that OT systems are communicating to the standards as set out in the SLAs with their customers.

The background of this dissertation will expand what is meant by IT and OT in the context of Eskom. The IT security component of Eskom seems to be very stable with many automated tools tracking and monitoring threat sources and has an awareness program which serves to educate staff about the multiple faces of cyber threats as they relate to information security. They are responsible for what we call the 'corporate' network. OT cybersecurity traditionally is very static with proprietary protocols running on segregated networks with little to no changes made in years. Patches are not done remotely or via a 'push' service, the operating systems are outdated and the focus is on availability, plant and human safety rather than confidentiality and integrity of information. New digital I&C (instrumentation and control) systems use similar protocols to operate and communicate on the same infrastructure as the IT systems and are now IP based. This is good for remote management and control, however with this new flexibility; OT is now exposed to similar risks as the IT environment. In the past, OT networks were completely segmented and often non-routable digital devices were implemented as part of the system design. This convergence has now exposed South Africa's electricity supply (which is classified a critical service) to emerging cyber-risks.

IT is entrenched in Eskom and has been set up to international best practice for IT service delivery utilising industry standards like ITIL, COBIT, and ISO 27000 to ensure that IT is managed optimally with appropriate governance structures, processes, technology and skilled resources. It would be reasonable to hypothesise that the level of maturity in terms of security culture would be far better than in the OT environment where the cyber threat has been evolving in the last few years (due to convergence) and the staff have an engineering focus with cyber as an emerging risk. Consequently they do not possess the depth of knowledge and support to deal with this emerging risk. Eskom has an information security department in IT, despite all the resources they have they do not mention culture in a single document, yet many elements of building a strong cybersecurity culture are being performed.

1.1 Aim, Objectives and Research Questions

1.1.1 Aim of the study

The aim of this study is to assess the level of cybersecurity culture by investigating how knowledge, attitude, behaviours and perceptions in the OT environment can influence cyber exposure of the enterprise.

1.1.2 Objectives

The research objectives of this study are to:

a) Contextualise the cybersecurity mandate with emphasis on the role of IT, OT and physical security.
b) Confirm whether user behaviour has an impact on the cyber-risk posture of an organisation (via literature).
c) Assess the cybersecurity culture of OT staff and comparing to IT, by investigating user attitudes and behaviour by developing an instrument for measuring this.
d) The results of the observations will be used to develop recommendations that will be incorporated into a program of work to catalyse cybersecurity transformation.

1.1.3 Research Questions

Do user behaviour and attitudes impact cyber exposure in organisations?

This aspect was dealt with by undertaking a literature review of existing material that highlighted the role of human error or judgement in organisations. There is a strong argument that while technical and automated controls like firewalls, encryption, SIEMs (Security Incident and Event Management) now coupled with machine learning algorithms are far superior when set up correctly to analyse and respond to the large volumes of data traversing a network, however this alone is not enough to keep an organisation safe. Human performance studies show that human error in industrial environments forms a significant risk organisations face. Industrial psychologists assist in developing an organisational culture by fostering strong team behaviour, accountability, integrity and trust and is a trait of a resilient organisation where employees feel like they are in it together [6]. Cybersecurity culture is often seen as a subset of organisational culture. We answered this question by undertaking a desktop study of existing literature on what the relationship of cybersecurity culture is on organisational risk and its threat landscape. There are many categories of cyber-attacks, some deploying remotely by breaching network vulnerabilities; others require some user interaction for example clicking on a link, opening an attachment, while others require physical access to a machine by accessing its USB ports as an example. Depending on the users perception of threats and their consequences there may be inadvertent risk created by ignoring good cybersecurity practice [7]. Users gain knowledge on cybersecurity by awareness and training programmes, policies and induction programs, but does this knowledge change attitudes and ultimately behaviour, or is it less organic? Technological controls of today are so advanced, integrating disciplines of AI (Artificial intelligence) that model the past and use machine learning (ML) to predict future actions, it begs the question whether it is good enough to catch all user errors and keep the organisation safe, or is culture transformation still required in the face of these incredible technologies.

What is the attitude and perceptions of staff toward cybersecurity in Eskom and how does this affect our threat landscape?

We aim to assess and evaluate user knowledge, attitudes, perceptions and behaviours based on four high level categories:

- Individual
- Processes and Technology
- Leadership
- Organisation

This assessment was performed by conducting a questionnaire of the organisation focussing on the OT and IT environment, and differentiated between business divisions, computer skill (personnel that have some kind of advanced computer training), demographics (age, gender), technical (OT and IT), non-technical, task grading. The questionnaire investigated how employees' knowledge, attitudes, values, perceptions and consequently their behaviour in OT supports a safe cybersecurity environment. We investigated how vulnerable employees perceive the organisation, whether technological controls in OT are adequate, how they conduct themselves outside of work and their practices in limiting their cyber-risk. It was important to investigate what processes employees use to report cyber threats, the level of commitment of leadership to cybersecurity and level of commitment of the organisation to cybersecurity. These questions focussed on the OT environment but the data gathered can be segmented to display the response from pure IT staff to see if there were any significant differences between OT and IT. We included some technical questions to verify knowledge levels versus how they answered a technical question. By asking users situational questions, and evaluating their responses we showed how our sample audience behaves and from this we can extrapolate the kinds of risks we are exposed to [8]. We left an open comments field as consultancies providing this service to Eskom believe that the best insights come from these comments.

Can an assessment of employee culture identify gaps in knowledge, attitudes and behaviour and can knowledge of this be used to transform cybersecurity culture in Eskom and ultimately reduce our cyber-risk?

By defining and measuring elements of cybersecurity culture in Eskom we were able to establish a baseline level of cybersecurity in Eskom's OT environment. Appropriate tools were utilised for analysis from which we gained insights, identified trends and patterns in the data. We then consulted with employees, managers and leadership and identified what influenced the patterns and trends we observed. During these discussions we uncovered drivers for behaviour and attitudes which we attempted to further analyse. From literature reviews, we confirmed this approach of baselining culture and utilised methodologies and best practice to develop and compare recommendations, identify metrics and implementation plans that will translate into awareness campaigns to increase knowledge and sensitise behaviour. By asking questions around perception of leadership, as an example, we can take the analysis of this and present this to Eskom leadership with possible recommendations to help transform the message and attitudes toward cybersecurity that employees experience. This can be integrated into the organisational culture programme that Eskom has, to have enterprise wide reach. This research is limited to cybersecurity culture and is not a full maturity assessment framework and methodology.

1.1.4 Ethics Clearance

Ethical clearance for this project was obtained from the Faculty of Science Ethics committee of the University of Cape Town (UCT) (see Appendix A). Approval was also obtained from the Security Solutions (Cyber) Department Centre of Excellence (CoE) Eskom. (See Appendix B).

1.1.5 Dissertation Outline

Chapter 2 is the literature review and highlights the similarities and points of departure between IT and OT. During the literature review, OT and IT will be contextualised in terms of the energy sector. Cybersecurity itself will be defined and the drivers and constraints from an organisational perspective will be explored. We aim to differentiate between information security and cybersecurity and mandates around this. Cybersecurity maturity models and implementation frameworks will be discussed leading to a sub aspect of maturity models namely, culture. Culture will be unpacked from information security and cybersecurity by examining literature around this topic. In order for us to see why culture is important, it would be expedient to unpack high-level cyber-risks and relate these if possible to culture and behaviours that may influence or even exacerbate the risks or opportunities possibly investigating actual incidents of cyber-attack.

Chapter 3 describes the methodology that was followed and will justify tool selection and execution. It will include questionnaire design, selection of questions, how scales were chosen, control questions, phrasing of questions and potential benefits of including an open-ended comments field. We will also expand on who was involved in the design and how it integrates into existing culture transformation initiatives.

Chapter 4 describes how the data was processed to prepare for analysis and will also list the results of the analysis. Respondents from non-technical staff will be used in a separate study by Group IT to influence programmes of work and training and awareness around information security. We will analyse the data and create summaries were possible in an attempt to roll up the detailed results into a summary report based on the broad areas identified: individual, leadership, process and technology, organisation and the intent is to transform the data to a numeric format upon which overall scores can be given to each. This can be used as a baseline for future questionnaires. Significant results may be used to influence future strategies, programmes of work and awareness campaigns as well as leadership training.

Chapter 5 will present high-level recommendations based on the analysis of the observations from Chapter 4. They should relate to the focus areas and have enough detail to inform a prioritised plan and eventually into a resourced programme of work.

Chapter 6 will conclude the research with a summarised statement of the intent of the study, the high-level observations and recommendations and whether the envisaged outcomes was achieved. It should also highlight any areas for future research.

2. Cybersecurity culture literature review

Chapter 2 elaborates on cybersecurity and how it relates to Eskom, while contrasting similarities and differences related to information security. There is further background and context of cybersecurity culture in the OT environment. Maturity models are also addressed at a high level and the emerging challenges of OT-IT convergence are further explicated. This Chapter also describes the regulatory environment in South Africa, with mention of any international legislation that may have an impact on us. This Chapter provides the theoretical background to be applied in the design and implementation of the questionnaire instrument, while highlighting trends, outcomes from research that can be used to understand the data collected from employees at Eskom.

2.1 Cybersecurity

Cybersecurity, according to the International Telecommunication Union (ITU), is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets [9]. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following (commonly referred to as the CIA triangle):

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality [9]

The International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC) defines cybersecurity as the preservation of confidentiality, integrity and availability of information in cyberspace [10]. While this definition encompasses the role of humans in cyber-risk and threat, however it does underplay the cyber-physical risks that utilities are susceptible to. The insider threat especially from disgruntled employees is a very real risk in the current political and economic climate [11]. Key in discussions related to the CIA triangle above we have found some fundamental differences between OT and IT focus. Martin Kuppinger discusses the conundrum of information being the asset versus plant being the asset. In environments housing critical infrastructure a higher premium is placed on safety, reliability and availability, with safety usually being paramount [12]. For example in a nuclear facility, nuclear safety is of the highest priority due to the long-term effects of ionising radiation. Reliability has massive impacts on continuity of supply with its associated financial implications. Availability of safety critical systems has a direct impact on plant safety as it deprives the operators of control measures that should be available when needed. This is supported by Eskom safety culture practitioners who the SSC CoE (Security Solutions Cyber: Centre of Excellence) have collaborated with, learning from their successes and failures. Bringing this back to cybersecurity, not having adequate patch management can expose vulnerabilities to threat actors that can render a system to perform in a dysfunctional state. The National Institute for Cybersecurity Careers and Studies defines cybersecurity as the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation [13]. The extended definition from the same institution refers to strategy, policy, and standards regarding the security of operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network

operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure [14]. The South African Cybercrimes Bill as expanded on in section 2.7 defines cybersecurity as technologies, measures and practices designed to protect data, computer programs, computer data storage mediums or computer systems against cybercrime, damage or interference [15]. It is the intention of Eskom to adopt the official definition from ratified legislation when promulgated. The National Cybersecurity Policy Framework (2015) describes national cybersecurity as a broad term encompassing the many aspects of electronic information, data and media services that affect a country's security, economy and wellbeing [16]. While this may satisfy national imperatives relating to data and media, Eskom will stick to the ITU definition that is more encompassing and relevant to the energy sector. Reegard, Blackett and Katta (2019) argue that "Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities" [17]. Cybersecurity, on the other hand, is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace" [17]. Reegard et al further state "In information security, reference to the human factor usually relates to the role(s) of humans in the security process. In cybersecurity this factor has an additional dimension, namely, the humans as potential targets of cyber-attacks or even unknowingly participating in a cyber-attack" [17].

ISO/IEC JTC1 (Joint Technical Committee) defines cybersecurity as "preservation of confidentiality, integrity and availability of information in the Cyberspace" [10]. The advantage of definitions based around confidentiality, integrity and availability (CIA) is that they keep open the potential role of humans in both cybersecurity risks, and protection from threats. However, CIA based definitions tend to underplay the potential for physical or insider threat risks as a component part of cybersecurity (e.g. deliberate sabotage of a key component in a power grid), either by cyber-attack or cyber-physical/insider threat exploit for example breaching the access control and installing malware or hardware that may compromise critical infrastructure [11]. There is still debate in OT circles as to the definition of cyber-physical threats; the one school of thought is where the physical and cyber world meet for example where a malicious threat vector gains physical access to a critical cyber asset and installs malware for command and control of the asset, similar to the STUXNET incident. The IT industry view cyber-physical threat as an emerging risk experienced by new generation physical systems like IIoT sensors, ICS', distributed control systems etc. that manage physical processes and the potential they have to be accessed and manipulated via cyberspace with potentially catastrophic consequences [18]. Due to the segmented architecture of traditional OT networks, most OT professionals consider an insider threat to be more likely than a remote cyber breach. This kind of attitude places the plant at risk as legacy equipment have little security by design. Some OEMs are now enabling integration of legacy systems into monitoring and control platforms that can be monitored across plant or corporate networks depending on configuration. While actual command and control of legacy equipment via this technology is limited, access to plant data is increased and could potentially provide intelligence to perpetuate an exploit.

2.1.1 Cybersecurity mandate in Eskom

Cybersecurity in Eskom was originally part of the Group IT portfolio, with the focus being on information security as per ISO 27000, COBIT 5 and similar information security standards. This aspect of the business is mature as best practice has been adopted and implemented, assessed, audited and continuously improved for a number of years in a very structured environment. With the formation of the Security Division in Eskom under Brian Molefe, previously the CEO of Eskom, physical and cybersecurity was supposed to be integrated into a single structure. Prior to this, some work was done at Eskom Research in Simmerpan under Engineering relating to cybersecurity of

operational assets. This work was specialised and very new and the team responsible for this was then moved over to the Security Division [19]. Studies and assessments were commissioned to evaluate the as is level of cybersecurity around operational infrastructure but a driver was needed to move this forward. With the appointment of General Rathabe as the Security Division Divisional Executive, a structure was created and ratified with a role for a senior manager for cybersecurity [20]. While this should have been an opportune appointment, as the cybersecurity agenda desperately needed a senior manager to drive it, it proved far more difficult to implement as IT security reported to the office of the CIO. The IT staff were not happy to move- even though by the very definition of cybersecurity as mentioned in the previous section it encompasses: tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment which includes IT security.

Even though in-principle agreements were reached, the co-operation and alignment between security and IT were not always fluid. Because cybersecurity was originally an engineering attempt at securing operational assets, Security Solutions then focussed on their original mandate with the focus on OT. After a business planning session in 2015, it was agreed that the senior manager for Security Solutions would have to ensure that the full mandate for cybersecurity was executed [21]. The SSC CoE has currently been re-instructed to update the cybersecurity operating model and are working closely with GIT to create a sustainable and optimised model.

2.1.2 Security differences

According to the National Institute of Standards and technology (NIST), cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation [13].

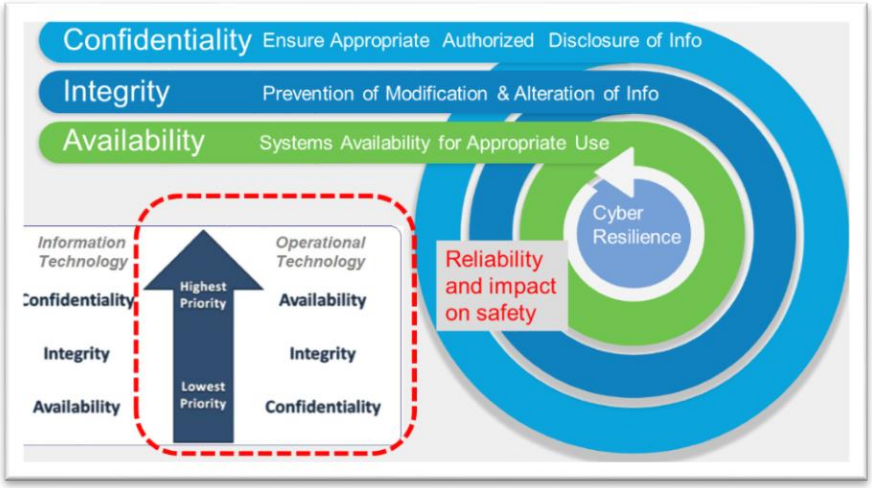


Figure 1: Diagram showing competing priorities in IT and OT (Eskom)

From the diagram above, IT security and OT security have similar focus areas confidentiality, integrity, reliability (CIA) but with different priorities [22]. Availability is of highest importance in OT as this affects reliability, which may have a direct impact on safety of plant and personnel. With IT security, the focus is more on confidentiality of information. Purists within the IT sector still segment security into Information security and IT security with information security focusing on the

strategic side of the business (frameworks, policies, risk, business continuity, GRC) and IT security focussing on the technical controls like hardware, incident response, vulnerability scans, DLP (data loss prevention), forensics, access control, network security.

In information security, information is the asset, in OT security the industrial systems and components are the assets and consequently the focus when it comes to securing these are very different. In OT, we face a number of challenges with respect to security:

- The lifespan of technology is historically between 15-20 years
- No security by design especially in the multiple legacy systems we have in operation
- There are limited cybersecurity skills in the OT environment
- There are unsupported operating systems in use where there are no patches being released
- Testing and patch management is challenging. Some legacy systems patches are a few years old. Due to the lack of interoperability, patches are done manually with no automation so there is no central way of tracking which devices are up to date [21], [22], [19], [23].

2.1.3 OT Cybersecurity incidents

Cyber-attacks on utilities and other industries using control and automation systems are on the increase [24], [1], [2]. The scale and complexity vary and technological controls are constantly evolving to meet the constant barrage of threat vectors like botnets, DDoS, malware attacks etc. Figure 2 shows a timeline of significant attacks on OT systems and it is clear that as we are embracing more digital technologies, the frequency and scale of attacks are also increasing.

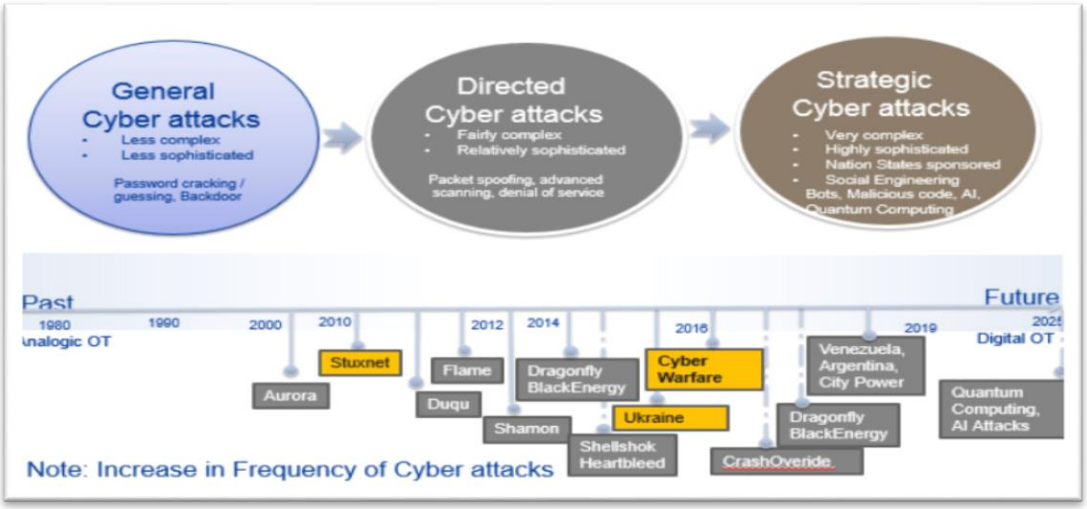


Figure 2: Timeline of attacks on OT Systems (ESKOM) [25]

Cyber threats follow many variants of a generic model [25]. The typical model looks similar to the one shown in figure 3. STUXNET and the UKRAINE Grid attack are probably the most prominent examples of large-scale OT attacks. South Africa being under the radar of world politics has so far

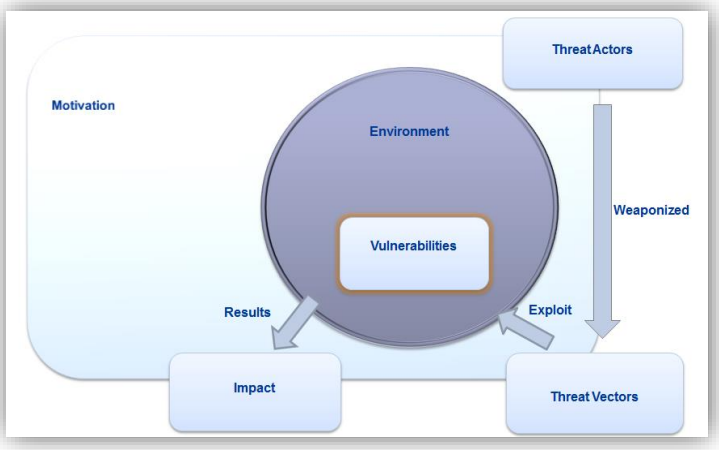


Figure 4: Cyber Threat Model (adapted Eskom) [25]

remained relatively unscathed from nation state attacks. Cyber threats follow many variants of a generic model. The typical cyber kill chain refers to a framework that was developed by Lockhheed Martin (the aerospace and defence corporation) for identification and prevention of cyber intrusions and is a model that defines the steps and techniques, techniques and procedures an adversary completes to achieve their objectives and is shown in figure 4 [25], [26].

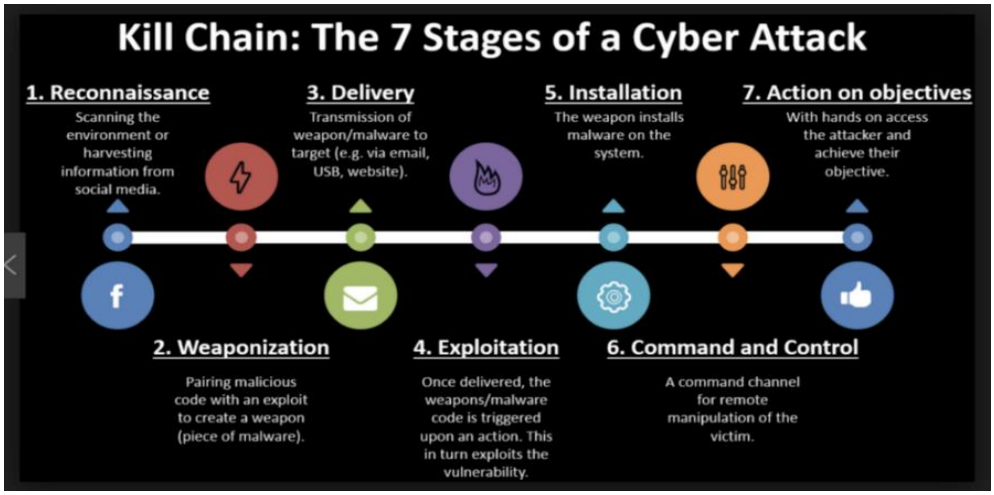


Figure 3: Typical cyber kill chain [25], [26]

In the case of the STUXNET (2010) exploit, there is widespread belief that it was a nation state attack involving the USA and Israel or a large organised hacking group against Iran and was perpetrated against the Natanz nuclear plant in an attempt to derail Iran's nuclear program [27]. The environment was scanned for vulnerabilities and once the threat actors knew what systems the plant was using they could then identify potential vulnerabilities. In this case the Siemens-designed centrifuges' PLC was the target and sophisticated malware was designed with a backdoor to infect the system. The plant was also accessible to third party contractor who delivered the payload via USB. The malware code once triggered would then begin to exploit the targeted vulnerability and open up a command and control channel while replicating itself on any linked PC but only activating if it found the Siemens SCADA module. This remote access then enabled the threat actors to achieve their objectives by discovery and updating the code where necessary. In this instance, the

centrifuges were allowed to spin beyond their design limits without sending a warning to the control room and this was only discovered when personnel walked past the room housing the centrifuges and heard the noise they were making which resulted in more than a fifth of the centrifuges being destroyed.

In this scenario there was a combination of factors that led to the exploit being successful; a vulnerability on Siemens S7-100/400 PLC, inadequate physical and logical access, employee negligence in allowing foreign devices onto the plant network, inadequate threat detection and prevention controls, not using a test environment before any updates are pushed, incorrect firewall configuration and an engineer using his personal laptop on a plant network. Many of these are linked to human knowledge and attitudes towards cyber-risk. Incidentally, it was the engineer's computer to which the virus had spread, that alerted them to the existence of the virus when he linked up to the internet at home due to a programming error in the malware. This exploit launched a number of security management programs with a multi-layered approaches often termed defense-in-depth and includes, policies and procedures, awareness and training, network segregation, integrated access control, physical security measures, patch management, system monitoring IDS (intrusion detection system) and IPS (intrusion prevention system) [27], [28].

The 2015 Ukraine power grid attack was allegedly orchestrated by Russian hackers who compromised the information systems of 3 energy distribution companies and disrupted the supply of power for up to 6 hours impacting over 230,000 people [29]. When looking for vulnerabilities across the organisations they realised that lack of awareness of employees, VPN configurations and threat detection and prevention systems were all entrance points. The attackers identified employees of the companies and used a targeted spear-phishing attack using malware in the form of an advanced persistent threat sent via email. Once the link was activated, a complex series of attacks was launched with hackers having remote access and being able to control SCADA (Supervisory Control and Data Acquisition) systems that controlled the grid. They also destroyed data on servers and simultaneously launched DDoS (distributed denial of service) attacks which all contributed to a large scale power outage [29]. This attack also leveraged human factors to gain a foothold, as it is usually the easiest way to gain access to a system. What is also noteworthy is that humans set up configuration on controls and in this case, the configuration was not set optimally which exposed the businesses to cyber-attack. Kaspersky in the state of industrial cybersecurity report 2019 found that 52% of incidents affecting OT or ICS networks in 2018 were caused by employee errors via unintentional actions [30]. The problem is exacerbated by a lack of skills, overconfidence in their skills to handle modern cybersecurity risks, no allocated cybersecurity budgets and misalignment in priorities of IT resources managing OT networks with OT engineers [31].

2.2 Cybersecurity Culture

This section deals with the psychological, behavioural and social aspects that influence culture and provides some basic theoretical background by exploring some behaviour motivation. Popular theories will be explained and used at a later stage to design the questionnaire that will help us establish a baseline for cybersecurity culture maturity. By comparing OT with IT, we immediately have an internal benchmark against which to measure. By including IT and other staff, we hope to gain some insight into IT security culture and will make recommendations based on the observations. We further contextualise culture in terms of cybersecurity and discuss its relevance to plant safety, availability and reliability and why it is needed in the face of intruder detection systems (IDS), intrusion prevention systems (IPS), unified threat management (UTMs), firewalls, processes and a myriad of technical controls. Organisations are at pains to describe the human element

correctly and are now making concerted efforts to not use phrases like 'the weakest link' or 'human weakness'. Insider threat often looks at humans as a liability rather than an asset but research shows that fear is not the strongest motivator of behaviour and positive reinforcement and empowerment has better results for behaviour change than punitive measures [11], [17].

2.2.1 What is cybersecurity culture?

While technical controls are very efficient at identifying, protecting and detecting cyber-attack, it has been noted that certain attack vectors like social engineering prey on human nature to open something without thinking, thereby setting a chain of events in motion. Spam filters can block up to 99% of spam but the 1% that make it through could have consequences especially if it contains malware [32]. In theory, a combination of anti-malware, whitelists and patch management should take care of this problem, but this does not always work. As an organisation grows in size with multiple sites with different operating systems, hardware and applications, this is not an easy task to accomplish and if a user mistakenly activates this malware, it can have major implications [32]. This human vulnerability has been widely acknowledged and many companies aim to mitigate this kind of risk by introducing organisation wide measures that target human behaviour, attitudes, knowledge and perception. Security departments must acknowledge that technical controls are never fully effective and need to employ holistic solutions incorporating people, processes and technology to maintain secure operations. According to Blacklett et al. [17] cybersecurity culture is understood as a subculture of organisational culture. While this may be so from their research, it is still a work in progress implementing cybersecurity culture transformation in Eskom, especially in the OT environment as it is considered to be a very specialist domain. According to ENISA (European Union Agency for Cybersecurity), cybersecurity culture is an organisations knowledge beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies [33]. I would also include 'and cyberspace' and remove 'information' in this definition.

At an organisational level Huand and Pearlson identified six management levers or constructs that can be used to influence cybersecurity culture shown in figure 5 [34].

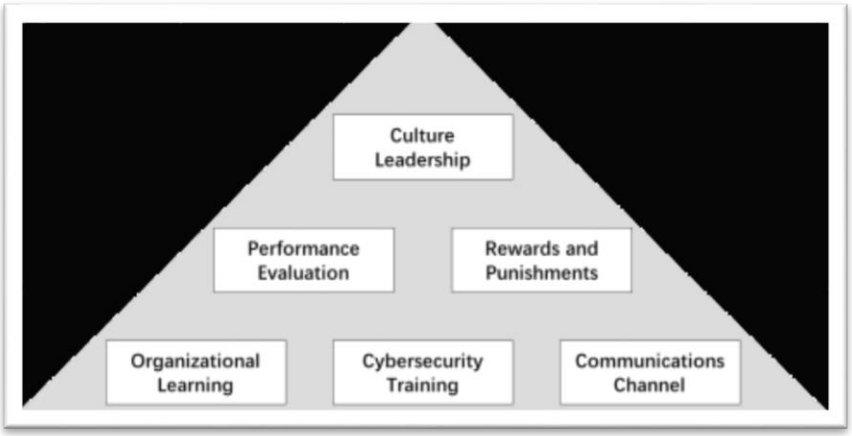


Figure 5: Organisational mechanisms for cybersecurity culture [45]

Batteau says that cultures cannot be managed in the conventional sense– but groups can be led, and if allowed space for growth, can evolve cultures [6]. Leadership cannot dictate a culture, but they can create goals and symbolic ideals toward which cultures can evolve. Leaders can present examples of integrity, and the spaces for employees and clients and customers to observe, try on and imitate- this leadership layer is very much ignored in most academic models that focus on the individual [6]. Top management buy in is seen as crucial to cybersecurity culture as seen in the

myriad references cited by ENISA and also supported by ISACA [32], [35]. It is interesting to note that this is also prevalent in Eskom and our culture transformation specialists focus on this extensively. Culture is a top down approach, a strategy and vision and plays a significant role in creating and propagating organisational culture [34]. People at grass roots level do not drive strategy and vision and it is extremely important to engage leadership and get their commitment on the transformation journey as they have organisational influence and control budget for initiatives. Besides, it is very difficult for staff to have great cybersecurity culture when leadership are not invested in it. According to Batteau, there are three measures of cybersecurity among leadership: priority, participation and knowledge and if any of these are missing, staff do not fully buy into the message [6]. We see this often in corporate space where leadership say that something is important, but do not commit any resources or effort into driving it, but if it shows up as an audit finding, then it becomes a priority until it is closed. This is also supported by Campbell [23] and Von Solms et al. who also highlight negligence, resistance and apathy as factors impacting commitment to compliance [36]. Unless that item affects the bottom line of profit or licence to operate it is usually not prioritised or resourced.

Schein (1996) defined culture as "a set of basic tacit assumptions about how the world is and ought to be that a group of people share and that determines their perceptions, thoughts, feelings, and, to some degree, their overt behaviour" [17]. Batteau examined people and their culture at various levels and concluded that at an individual and group level they are two separate though related problems. Human factors (training, skills, attitudes etc.) are described as dimensions at an individual level, but at a group level we are concerned with norms, shared values and commitments [6]. Organizational culture is described as having three levels: tacit assumptions that are beliefs about reality and human nature; espoused values which refers to social principles, philosophies, goals and standards; and artefacts that are visible, tangible, and audible results of activity grounded in values and assumptions [17]. For cybersecurity some researchers have added a fourth layer for knowledge, arguing that knowledge will influence the assumptions, values and behaviours [33], [37]. Figure 6 illustrates the proposed layers in cybersecurity culture [17]. There is a strong link to the KAB (knowledge attitudes behaviour) model as described by Parsons et al. which states that as knowledge of safe work behaviours in the workplace grows, there is an improvement in attitude which can translate into safer behaviour [38]. Organisations with a high emphasis on safety (nuclear, airlines, naval) are in a constant state of training and this ensures continued vigilance [6].

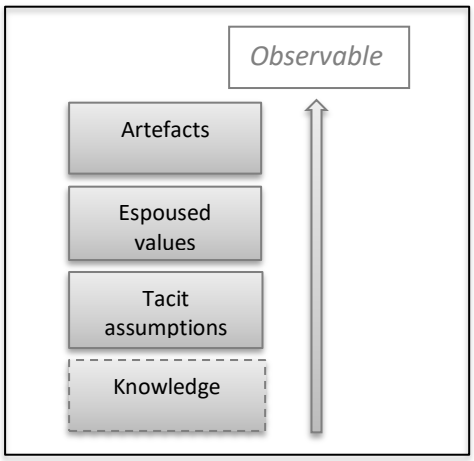


Figure 6: Organisational mechanisms for cybersecurity culture [45]

Generally behaviour is not changed by just changing a single variable but is influenced by different aspects, like fear and protection, societal norms, values and the desire to fit in; knowledge and

awareness of a risk, creating awareness to enable coping with a cyber-risk. Knowledge and awareness while being a prerequisite of behaviour change is not enough to change culture, it needs to be implemented with other influencing strategies. It is also important to embed positive cybersecurity behaviours, which results in habits and positive change [39]. Huang and Pearlson further expand on this model to include organisational mechanisms and external influences that affect beliefs, values and attitudes and in turn cause certain behaviours and like Batteau, separate culture into layers focussing on the individual, groups and leadership [34], [6]. Group constructs include community norms and beliefs, teamwork perception and inter-department collaboration [34]. At an individual level constructs similar to information security and aligning to behaviour motivation theory include self-efficacy, policy awareness and cyber-threat awareness.

There are two behavioural theories that will be described as they form the basis on which many cybersecurity culture studies are based. These attempt to understand what drives behaviour change, but by far and large the bulk of studies have looked at Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), COM-B and Fogg's behaviour model are useful in establishing causes of unsecure cybersecurity behaviour [33]. Although the focus of this research is on establishing a baseline for cybersecurity culture, these behaviour change models, will be crucial in helping analyse how we develop interventions at a later stage by decoding the drivers of behaviours and attitudes observed. ENISA have conducted an in-depth analysis of over 600 articles and summarise the findings related to cybersecurity culture [11]. The evidence reviews were categorised into those based on social science constructs, attitudes and behaviours, qualitative and mixed methods and current practices.

The next few paragraphs will focus on the outcomes of the summary performed by researchers at ENISA and of note is that while the title refers to cybersecurity culture it has a strong focus on information security culture [11], [33], [40], [41]. Social science constructs refer to research that was based on behavioural science theory using variables that are not directly observable like attitudes and personality and are assumed to influence human behaviour in cybersecurity resulting in compliance with policies. The variables were tested by creating targeted awareness programmes or behaviour modification exercises. After implementation of these, the employees were then again assessed and the results from these used to determine success. Some commercial culture change solutions use this approach as it is very simple to measure and focuses on a single variable at a time and does a before and after assessment. From these reviews, ENISA found that there were 92 categories and 984 constructs of which 789 were unique that were used related to cybersecurity behaviour [11]. This large number of constructs raises questions regarding validity, correlation, causality and we question if a systemic based approach may not be more suitable for modelling behaviour and its drivers.

Safa et al. measured responses to information security knowledge sharing , collaboration, intervention and experience, attachment, commitment, personal norms and attitude to information security compliance and intention to comply with information security policy and is based on social bond theory [36]. The overall results identified that a lack of information security awareness and training, ignorance, negligence, apathy and resistance are the root cause of the users' risky behaviour. These studies used inferences and correlation as direct drivers but without testing causality. This is a limitation of models and constructs in that they often ignore underlying factors and root causes, for example, there is no mention of how processes or even leadership impacted behaviour. This is understandable however, as academic research try to isolate factors that can affect behaviour. There is also a more encompassing view of adopting a systems approach. Eskom has been teaching leadership how to adopt a systems approach, which is a structured approach of

dealing and understanding complexity. The Information Systems Audit and Control Association (ISACA) have also included this approach as part of their CISM (Certified Information Security Manager) certification by including the Business Model for Information Security (BMIS) [42]. Once a baseline assessment is done using qualitative methods, it can be further fine-tuned to deep dive into the factors driving behaviours and attitudes. These drivers can then be addressed by campaigns and evaluated for efficacy.

The second category of review performed by ENISA was on research that looked at how attitude predicted behaviour and the human factors that reliably influence these. The majority of these relied on self-report measures of cybersecurity behaviour or intention to behave. These could take the form of simulations or exercises, analysis of password selection, backing up and passive data collection collected from user activities for example not allowing pop-ups that appear. However self-reporting does not always correlate with actual behaviour. The Protection Motivation Theory (PMT) and Theory of Planned Behaviour (TPB) models were used in many studies in both social construct studies, and attitudes and behaviour studies and will be described now. PMT is linked to risk management and proposes that people protect themselves (or their organisation) based on the severity of a potential threat, likelihood or probability of the vulnerability happening, perceived or actual effectiveness of the recommended preventative and effectiveness of employee response (self-efficacy) at implementing the recommended preventative behaviour [43], [44]. It also mentions response costs, which is the cost of responding and can be physical or psychological. Many studies have found weak, neutral or negative relationship between increasing threat appraisal and motivation to take protective action or act securely, and models based on this theory don't have a high propensity at predicting behaviour or even significantly transforming behaviour [33], [45].

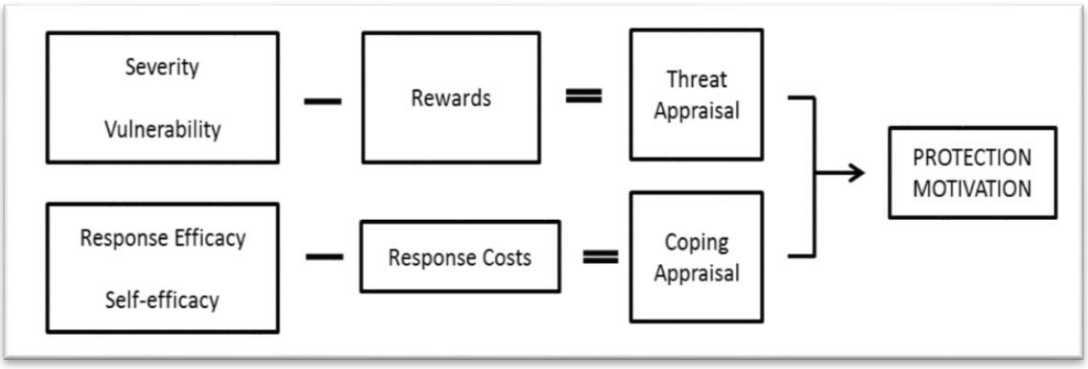


Figure 7: Protection motivation theory [44]

Figure 7 represents PMT in the form of an equation. Eskom's integrated risk management (IRM) programs not only view risk as a threat or vulnerability but also as an opportunity that supports this theory. There is a fine line though, as fear is sometimes linked to risk, but as a motivator to change behaviour, it will be less powerful than increasing a person's ability to identify and rank a threat and equip them with the knowledge to deal with it. The Theory of Planned Behaviour (TPB) links belief to behaviour and focuses on coping and enablement as shown in figure 8 [44], [11]. It states that intention toward attitude; norms and perceived behavioural controls together shape an individual's intended and actual behaviour and has been very successfully used in marketing and sales. Human behaviour is guided by 3 considerations: behavioural (linked to intention), normative (societal or group behaviour) and control beliefs (linked to performance and self-efficacy) and these three considerations ultimately leads to behavioural intention, which may or may not lead to behavioural action hence the name 'planned' behaviour theory. Behaviour is an individual's observable response to a given situation and according to Ajzen who developed the TPB he says it is a function of

compatible intentions, perceptions of behavioural control where behavioural control moderates intention and favourable intention produces actual behaviour when perceived behaviour control is strong [11], [39]. In simpler generic terms, perceived self-efficacy of performing a behaviour moderates the readiness to behave in a certain way and only produces actual behaviour when you feel confident that you can perform in the recommended way. If one of these constructs is unfavourable then you may not perform the behaviour, if two is unfavourable the probability decreases even further. Both models also ignore processes, technology, leadership and organisational influences and feature compliance very highly.

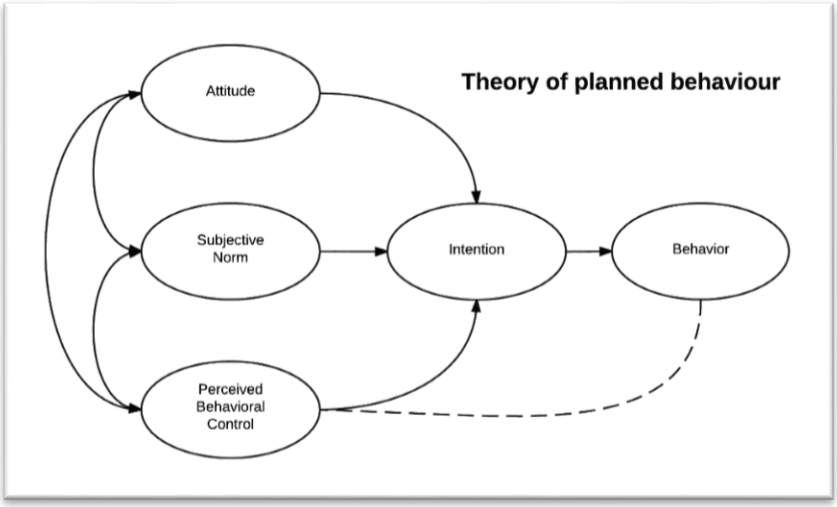


Figure 8: Diagram of theory of planned behaviour [50]

From a human psychology perspective, staff may change their behaviour if they are dissatisfied with the current cybersecurity culture and if this causes anxiety or guilt. This may still not be enough to change behaviour as they still need to be sure that they can do this without compromising their identity or integrity [46], [33]. Awareness needs to target the types that do not adhere and figure out the circumstances and underlying values that drive the behaviour. For compliance or adherence, employees' perception of cyber-risk needs to change and they need to understand their role in adhering to policy as this will keep them safe from potential attacks. This is an indication of how mature the cybersecurity culture is, for example if you conduct a phishing exercise, the employee can either act insecurely by clicking on the link, or he could delete it, or if his culture is advanced, he can choose to report it [32]. Rewards can be used to motivate and reinforce secure behaviour however there should also be a degree of coercion as consequence is also a driver of human behaviour [47]. There have been a few studies like those done by Ashenden, Beautement , Kirlappos that used a mixed approach of observation and interviews where factors influencing behaviours were first identified and rather than applying a theory of what drives risky behaviour they attempted to understand the causes of non-compliance and this formed part of a multistep program [48], [11]. Eskom wants to adopt a similar approach as we realise transformation is not a single step solution with immediate results. Some of these studies linked attitudes and behaviours through related attributes. Ashenden, in her PhD thesis, described awareness campaigns that segmented employees into 'I can handle it' and 'It's out of my control' group and was done using multiple interventions with more targeting as the process progressed [48]. This also links back to efficacy in TPB model described earlier.

The most common quoted driver for non-compliance to policy was complexity of control versus production pressures [39]. Eskom experienced a similar phenomenon with the implementation of MS Azure for data loss prevention (DLP). Besides the impact on system performance, there was a

misalignment in information security classification processes and lack of understanding of the documentation standards which either resulted in unnecessary protection that was too stringent or a lack of protection because the service was disabled or the user could not clearly find the correct option. This led to large scale non-usage of the tool as we found that employees fear more the consequences of low production over non-compliance that could lead to a cybersecurity incident and is support by results from Kirlappos [49].

Generally security metrics come from measuring compliance against a policy or standard, cost of security either from impact of incidents or actual money spent on investments, effectiveness measuring from initiatives implemented [13]. There is increasing evidence that threat and fear on its own does not change behaviour and needs to be couple with skills and tools for there to be behavioural change [39]. There should be a drive from compliance to adherence as it implies a proactive attitude emanating from the employee, which is supported confidence in their abilities and the desire to protect the organisation. This can be achieved by improving communication, trust, collaboration and embedding cybersecurity into work processes [48]. However, trust may be compromised if there are no cyberattacks and fear is the main driver of a culture change initiative. ENISA advocates a blended approach based on organisational behaviour assessment using the different motivation theories across various levels in the organisation and involving different functions like organisational culture and training. It's also important to note that human issues have underlying drivers and it is important to understand those and it could be a knowledge gap, technology breakdown etc. According to ENISA's study on organisational cybersecurity culture, behaviour change can be effected if cybersecurity forms part of work processes, is supported by policy and strategy, if leadership is committed and actively supporting the culture change, supporting technology and clear metrics and communication [33]. Even with all these, it is not an overnight process and there needs to be equilibrium between people, processes and technology.

As cybersecurity essentially deals with risks, it is frequently emphasized that cybersecurity is a continuous process of identifying, assessing and responding to risks [33], [50], [51]. Consequently, a mature cybersecurity culture is associated with fostering security awareness, risk perception and being sensitive to changes in threats. The beliefs regarding humans and their behaviour in cyberspace is a highly relevant assumption when addressing cybersecurity culture. Different approaches to reducing the insider threat can be related to the organizations' belief regarding humans as a liability versus an asset in cybersecurity: to ensure technical controls to reduce or mitigate the risks posed by employees, or to focus on empowering the employees to contribute to the organization's resilience [17].

From as early as 1975, psychology, human factors and crime science were included albeit to a very limited extent in the protection of information systems [52]. While the focus for the most part have been on technical controls, the human element was modelled via system policies, processes and administrative controls. Other technical controls like whitelisting and rules based policies work well for known exploits that follow known patterns. However, for human vulnerability, these measures are largely ineffective. Eskom implemented a data loss prevention (DLP) solution and introduced product training via eLearning, only to find that users still did not classify information correctly and stopped using the solution. Interactions with Group IT indicated self-efficacy, process understanding and performance as drivers to non-usage, relating closely to the theory of planned behaviour and protection motivation. Another example can be a firewall which if configured correctly, can be very effective at screening out potential attack vectors, however if the person configuring the system uses the incorrect parameters, can either cause unnecessary breaches or loss of business due to overly strict policies screening out information that is important to operations. These reasons

highlight again that humans are a real vulnerability but the reasons as to why change interventions fail can vary. If cybersecurity is viewed as critical to business operation, then the organisation will strive to balance the attainment of business objectives and cybersecurity objectives.

2.2.2 Cybersecurity culture in OT and its transformation

In the past critical infrastructure culture focused on safety, performance and security culture as safe production was top of mind for most plant environments. The majority of stakeholders in these environments viewed cybersecurity as a low priority goal, relying on security via obscurity/secrecy to ensure protection [53]. Obscurity and secrecy worked well for first and second-generation systems, however third and now fourth generation systems more frequently use open technologies, while communicating over non-OT networks increasing the attack surface substantially. There is also a lot of information relating to legacy and modern ICS' in the public domain which was previously only accessible to people working in the industry rendering obscurity and secrecy as a defence strategy ineffective. Traditionally cybersecurity in ICS' used AIC (availability, integrity and confidentiality) as opposed to the CIA triad in terms of priorities. ENISA has introduced an alternative way of looking at security called SRA (safety, reliability, availability) that more closely aligns to plant priorities [41]. Piggin presented the following challenges for OT cybersecurity and specifically these that can impact cybersecurity culture: the challenge of merging IT and OT elements of risk, accountability for OT cybersecurity, governance structures, cultural change, IT-OT collaboration, developing OT cybersecurity competency [54]. This is supported by Knowles, Prince, Hutchison, Disso and Pagna (2015) who also acknowledge misaligned security goals (CIA) between IT and OT as a challenge and suggest that security management cannot be directly implemented from information security [53]. They further also highlight the fact that operational security is not adequately addressed in information security. ICS safety refers to safe plant operation within design parameters and security deals with reducing the risk of cyber or physical attack. Fail-safe is a core principle in ICS design and focuses on human, plant and environmental safety and always has a higher rating than a fail-secure state which is of higher priority in IT [53]. This is also used as a counter argument to cybersecurity controls by OT personnel when challenged on cybersecurity transformation- with the argument that if there is a cyber-breach, that there are fail safe procedures in place to recover the plant an example of which is the ability to disable digital systems and switch to analogue.

Security metrics play a role in measuring cybersecurity maturity and the efficacy of controls (administrative, procedural, technology, physical) and there are benefits in adopting a combined defence-in-depth approach to deal with cumulative and cascading impacts. Another key issue is establishing the best way to stimulate change in the organisations culture [53]. Most organisations first step in this journey is to establish a baseline of what the existing culture is using a tool, existing metrics, observations or a combination of these approaches. Once this is measured and gaps identified, culture transformation is addressed typically using training and awareness. Awareness programs are usually the same across the enterprise, but training is usually focussed and can span basic right up to advanced levels depending on the function of the department, organisational level and audience needed to be engaged. A high dependence and confidence in technology can create a human factor vulnerability as staff take unnecessary risks thinking that technical controls are fully effective. It is up to management to institute a culture of cybersecurity and this message must infiltrate to the most remote points of the organisational flow chart [35]. According to the Anti Phishing Working Group, there were over 1,220,523 phishing attacks in 2016, an increase of 65% over the previous year with over 9.2 million suspicious emails reported in 2019 via Phishalarm [55]. It is widely accepted that it is harder to breach network security than to trick an employee, hence it is one of the most popular attack vectors of cybercriminals with novice to expert knowledge [32].

There is the view that spending money on technical controls is far better than wasting it on awareness and training [32] especially in the OT environment as the managers are accountable for physical processes and find it hard to deal with 'soft' controls. Cybersecurity in OT is often seen as an IT problem, and understanding security is not the same as practicing it, hence awareness is not effective and requires more creative ways to change security behaviours.

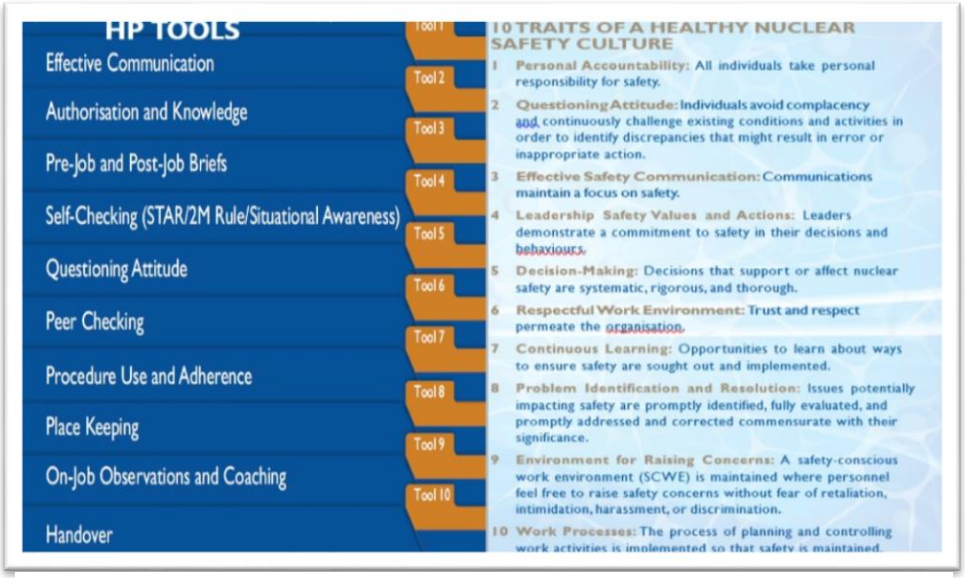


Figure 9: HP Tools and Nuclear Safety Culture Traits (Eskom) [57]

Good metrics is important to show return on investment (RoI) on cybersecurity awareness and training and it is extremely important to obtain executive sponsorship [32], [33]. "Only by investing in employees, rather than attempting to take them out of the equation, can a security-conscious enterprise flourish in the coming years" [32]. Safety culture is an important part of the OT environment and in the nuclear energy sector; nuclear safety is the highest priority, even trumping production pressures. There are many nuances and lessons learnt from safety culture implementation that can be used in the transformation of OT cybersecurity culture. Having a good safety culture does not mean that employees are overly cautious, but that they are prudent and knowledgeable often with tools to help in difficult situations [54]. These are sometimes called human performance tools and examples are STAR (stop, think, act, review), 2M (2 man/metre) rule and relates to situational awareness, pre-job briefs, place keeping, peer checking- a total of ten tools in the nuclear environment [56]. For nuclear safety culture, there are nuclear traits that are defined and measured and shown in figure 9 and include personal accountability, questioning attitude , decision making and so on [57].

Defence in depth is another popular concept in OT and is the opposite of a single technology solution but is comprised of multiple and consistent controls (policies, procedures, technologies, processes, trained personnel) that work together in layers so that if one is breached there are others in place afford protection [6]. Becoming a cyber-resilient organization is a combination of both technology and organizational investment [34]. Awareness and training needs to be targeted, actionable, doable and feedback driven. Once people want to change continuous feedback is needed throughout the change period and cognisance needs to be taken of the various cultures and knowledge levels [39].

A new British standard, PAS 555:2013, Cybersecurity risk – Governance and management, takes a different approach, offering organisations a scalable approach that engenders an understanding of the capabilities required [21]. The framework emphasises that technical measures alone are not

sufficient; effective outcomes encompass people, behaviours, physical equipment security, governance, leadership and culture. PAS 555 defines the fundamental outcomes that specific security practice should achieve, rather than how to implement them, understanding that the appropriate measures are likely to change rapidly over time. Whilst the standard recognises the need to specifically address ICS vulnerabilities in building control systems, industrial process control and manufacturing, it does not reference guidance for ICS security implementation [54]. NIST has a framework for improving critical infrastructure cybersecurity. It is outcomes focused and technology agnostic and has been adopted as a standard against which Eskom measures cybersecurity maturity. IEC 62443 are based on ISA-99 technical reports and focus on cybersecurity of industrial automation and control systems. It quite clearly differentiates between IT and automation and controls systems.

2.3 IT Security

While OT focusses on operational assets and their security, IT security focus is on the protection of information and its integrity, availability and confidentiality. IT is a common term used to describe a large spectrum of technologies used for corporate information processing including software, hardware and related services and also includes unified communications systems. Eskom structure has a Group IT department that looks after all Eskom information assets, hardware, software reporting to a Chief Information Officer (CIO). Part of this structure is the Information Security Department that looks at information security risk throughout the business. In the past, the domain did not look into OT assets and their security but rather terminated at the junction where IT networks interfaced at the OT network [21]. It is increasingly obvious that prior governance and collaboration practice was not adequately tuned to leverage off each other. The technology advancements, adoption of similar platforms, infrastructure and common communication standards are creating opportunities for interfacing and collaboration between IT and OT systems.

SANS defines Information Security as the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption [58]. SANS further describes it as the practice of protecting information by mitigating information risks and is part of information risk management. It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection, recording or devaluation of information, although it may also involve reducing the adverse impacts of such incidents. Information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity [59]. Eskom has segmented its network infrastructure into two namely the IT or corporate network and the OT or operational technology network. These have very different functions and have very clear logical and physical separation between them. Purists within the IT sector still segment security into Information security and IT security with information security focusing on the strategic side of the business (frameworks, policies, risk, business continuity, GRC) and IT security focussing on the technical controls like hardware, incident response, vulnerability scans, DLP (data loss prevention), forensics, access control, network security [58].

Information security culture acknowledges that the human factor plays a significant role in information security risk and is usually approached at a strategic level as culture is widely regarded as a top down initiative. Employees at the operational level will not influence policy and direction setting, this is done by top management (usually a CISO if the structure permits). Questionnaires

conducted by PWC in 2013-2015 indicated that human error and not technology is behind most of security breaches investigated [60]. This is supported by IBM global technology Services who report that 95 percent of security incidents investigated expose human error as a factor in the incident [38].

Information security culture is seen as subset of organisational culture and should align to the organisations culture. The corporate culture guides the organisation and its employees by placing constraints on the actions and behaviour of its people [61]. Da Veiga as quoted by Hogail & Mirza defines information security culture as the way things are done in an organisation to protect information assets [60]. There are various international frameworks like NIST, ISO 27001, ISF, and COBIT 5 [62], [47], [53], [13], that deal with cybersecurity or information security maturity with culture being one of the elements of the frameworks . Others like the organisational culture framework adoption of Detert, to an adaption as described by Schlienger and Tuefel which is loosely based on ISO 9001 quality management principles of the PDCA (Plan-do-check-act) and has five main phases: pre-evaluation, strategic planning, operative planning, implementation and post evaluation [60]. ISO 9001, moves towards a culture of continuous improvement and advocates a cyclic approach which moves beyond post evaluation phase [63]. CISM and ISO 27001 both advocate the performing of a benchmarking or gap analysis exercise as part of the evaluation phase and can be done by evaluating the gap between the InfoSec policy and the perception of employees or their compliance to requirements. The operative planning engages management and development of awareness and training programmes. Implementation has four stages from management commitment, communication programmes, knowledge transfer and employee acceptance. Schlienger & Tuefel also go on to define information security culture as the values, attitudes, know-how and patterns of behaviour that determine the commitment to information security [63].

Chang & Lim evaluated organisational culture traits like cooperativeness, innovativeness, consistency and effectiveness and its relationship to information security management [64]. Lim et al. drew a relationship between the organisations threat profile and its organisational culture with a low threat profile allowing a separate InfoSec culture, medium threat landscape requiring ISC (information security culture) to be a sub culture of organisational culture and if the organisation had a high risk security profile to have ISC embedded into the organisational culture [64]. Da Veiga and Eloff developed a comprehensive information security framework (CISF) that looked at people process and technology and how these affect establishing of an ISC [65]. These components are linked to individual, group or organisation tiers and they evaluate how employee behaviour is linked to these tiers. A possible shortcoming is that they do not look at perception of employee to these tiers and ignore aspects of leadership [65].

Awareness programs need to address gaps that are found based on the analysis of process, people and technologies that support information security but specifically focussing on the human aspect. Parsons et al. have found that awareness programs focus on two aspects; the first is on how well do employees understand what is safe information security behaviours as outlined in their processes and procedures (this will include policies, guidelines etc.) [38]. The second aspect deals with the extent to which employees are committed to an idea and how they behave based on this commitment. It is based on the KAB model (Knowledge-Attitude-Behaviour) [38]. A similar model is presented in cybersecurity culture as described by Blackett et al. [17]. Questionnaires are a popular way of assessing behaviour but most models focus on a single area and hence give very limited results. Some behavioural models used in various studies include the General deterrence theory, protection motivation theory, theory of planned behaviour and health belief model [36] [38] [11] [66]. Choosing any one of these models limits the scope of the analysis as only one major variable is investigated. Ögütçü, Testik and Chouseinoglou presented four scales to measure computer related

security behaviours and awareness levels namely the Risky behaviour scale, conservative behaviour scale, exposure to offence scale and risk perception scale, but has not been adequately tested for reliability and validity [66]. Parsons et al. have developed a robust framework to compare 7 focus areas (Password management, email use, internet use, social media use, mobile devices, information handling, incident reporting) against the KAB model with 3 sub-questions per focus area with each one having a question from a knowledge attitude and behaviour perspective [38]. As seen in table 1 below, the questionnaire can be adapted to emerging technology quite easily, but has no dimensions for organisation and leadership, which are critical components of culture.

	Knowledge based question	Attitude based question	Behaviour based question
Password Management			
Email use			
Internet use			
Social media use			
Mobile devices			
Information handling			
Incident reporting			

Table 1: Framework for human aspects of information security questionnaire

This research observes that while table 1 addresses the individual aspect of a culture transformation, it ignores the most important aspect, in that culture transformation is a top down approach and ignores leadership and direction setting as the most critical part of culture transformation. This tool would be suitable for assessing an as-is individual state. It is therefore essential to consolidate the best of the different approaches and tailor a solution to fit your organisation.

2.4 Operational Technology

Operational Technology (OT) refers to the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, actuators etc. Simply put, OT is the use of computers, analogue or digital devices that monitor or alter the physical state of a system, such as the control system for a power station or the control network for a rail system. The term has become established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment, the so-called "IT in the non-carpeted areas". Examples of operational technology include:

- PLC (Programmable Logic Circuit)
- SCADA (Supervisory control and data acquisition)
- DCS (distributed control system)
- Computer Numerical Control (CNC) systems, including computerized machine tools

- Scientific equipment (e.g. digital oscilloscopes) [67]

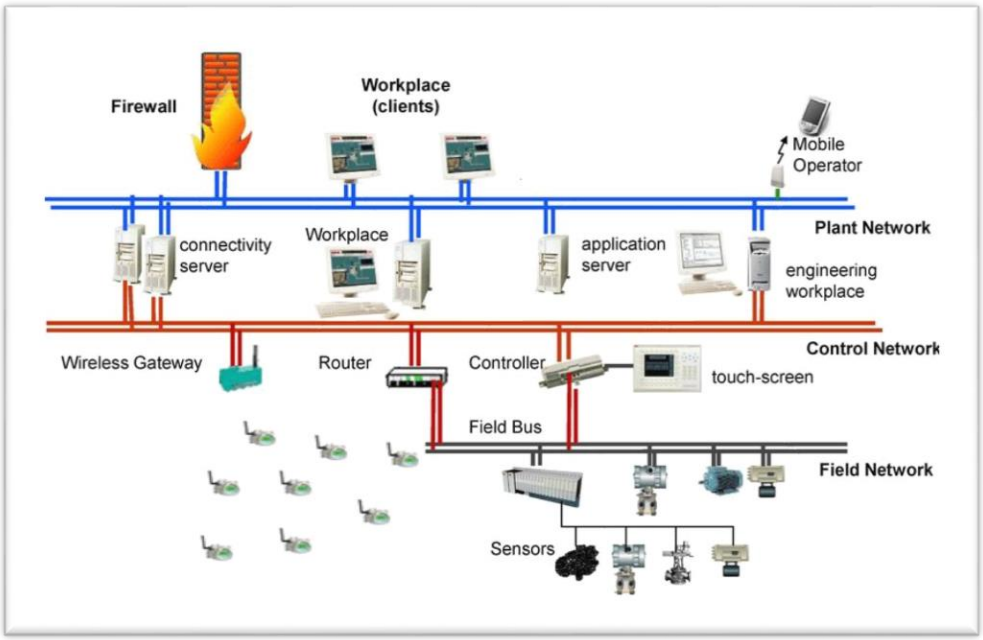


Figure 10: Industrial Control System example [8]

Figure 10 shows a basic ICS showing three subnetworks namely the field network, control network and plant network. The field network typically has measurement and sensor devices (optical, magnetic, thermal, etc.) to measure temperature, pressure, voltage, etc. The field network could also contain IoT devices that link to the control network, though generally frowned upon and also referred to as IIoT (Industrial Internet of Things). While this is feasible in theory, it is considered too high risk from a cyber threat perspective for most plant environments and may only be feasible in non-critical semi-automated environments.

The control network manages the field devices and sensors and typically contain remote PLCs, RTUs (remote terminal units), servers and controllers that acquire data from sensors and actuators. The plant network is made up of a number of servers for connectivity, applications (vendor and internal), monitoring, controllers, workstations, concentrators etc. This network also have proprietary communication protocols that are sometimes non-routable and non-IP based. New technology has introduced IP based solutions. Examples of plant system protocols are Modbus, RS-232, RS-485, PROFINET, DNP3 etc. Some of these are proprietary to the vendors [68]. As can be seen above, all this technology is separated by air-gapping, configuring of a DMZ (demilitarised zones), or at a minimum with a firewall with strict exception rules allowing only one-way communication.

Group Technology in Eskom has the mandate to ensure that there is technical support provided to the business that allows Eskom to operate and maintain the asset base in a safe, standardised and optimal way to achieve first quartile availability. By ensuring there is sufficient and efficient availability of engineering resources and structures to mobilise and engage with business, Group Technology makes an impact on standardisation and smooth operating of the utility. One such structure is SCOT (Steering Committee of Technology) which focuses on the development of enterprise wide standards, one of which is cybersecurity for the OT environment. While the care groups and study committees usually comprise engineers and staff working in the environment being studied, the onus is on that coordinator/chairman of the various workgroups to ensure that adequate coverage is present and all major decisions are ratified only if a quorum is present.

Representatives typically from all areas of the business example Transmission, Distribution, Generation, IT and so on would need to be co-opted as standards and best practice rolled out specify minimum requirements applicable throughout the enterprise. The reason for the preamble is that most Eskom documents referenced in this report are confidential and hence not available on any public platform. They also peer reviewed internally and sometimes externally following a very stringent configuration and change control process, so where quoted in this report, the credence given to it should be the same or if not at a higher level than academic literature [69].

In Eskom, Operational Technology (OT) Systems are defined as follows: Operational systems which form part of Eskom's plant / network assets, and which could by virtue of design, maintenance or operation directly result in the failure of these assets to meet their purpose and performance criteria, where:

1) **Operational systems**: are all systems (including electronic, telecommunications and computer systems and components) which process, store or communicate operational data or information.

2) **Part of**: means contribute to the asset meeting its purpose and performance criteria.

3) **Plant / network assets**: are any part of the "built environment" utilized by Eskom to run its production, delivery and logistics processes, including generation, transmission and distribution of electricity, etc.

4) **Directly**: means in real time or near real time. E.g. would include supervisory control systems, but would exclude spares ordering applications (even though these could eventually result in the failure of the asset).

5) **Purpose and performance criteria**: The "design to", "maintain to" and "operate to" criteria that are generally specified formally [20].

Systems, sensors, transducers and Programmable Logical Controller equipment, which extract signals and measurements from the plant or network asset or its control environment, or facilitate control over these assets generally meet the above criteria and qualify as OT. Further, their failure could directly result in the failure of the plant or network asset or its ability to meet its purpose and performance criteria.

In some cases, obvious failures of operational systems may not directly result in the failure of purpose or performance of the plant or network asset, but because of the way it is designed, normal operations or maintenance of the operational system could result in a risk to the plant or network asset. An example of this is a voltage spike induced in a control circuit due to a lightning strike on the power supply of an IT server not fitted with the same spec of surge protection as used on the control circuit, and inadequate voltage supply decoupling (e.g. optical decoupling).

Such equipment generally meets the above criteria and qualifies as OT, since their design, operation or maintenance could directly result in the failure or impact of the plant / network asset or its ability to meet its purpose and performance criteria" [70].

2.5 OT-IT Convergence

OT has historically been in the realm of control and monitoring systems developed and supported by engineers responsible for maintaining the integrity and performance of electrical plant and associated engineering networks also referred to as Industrial Control Systems (ICS). Generally, IT and OT did not integrate well due to technological differences, proprietary communication protocols, platform differences, availability requirements and related safety requirements. With

technological advancements, increased calls for standardisation, interoperability and common communication standards, there are increasing opportunities for interfacing, collaboration and data exchange. With this convergence, the level of risk posed to OT has increased and the need for a collaborative approach is of critical importance in the current threat landscape. The IT domain typically sees performance, confidentiality, availability and data integrity as paramount, while the OT domain views human and plant safety as primary responsibility, thus system availability and integrity are its core priorities [71].

The Eskom IT-OT practice note [20] highlights the following trends that are infiltrating the OT environment:

- Underlying platforms are analogous
- Shared infrastructure, standards and approaches
- Shift from proprietary hardware based to software based technology
- Evolution of new risks introduced by software based technologies
- Adoption of these trends to remain competitive.

Emerging technologies like IIoT (Industrial internet of things), Smartgrid, industrial Wi-Fi networks, IP based routing are introducing vulnerabilities never before experienced on a segregated industrial network. Research by Gartner in 2017 identified a few trends that Eskom is already grappling with:

- For organisations managing both IT and OT, these have always been separate functions. Over time, there may be a measure of merging dependent on regulatory compliance and organisational maturity. For example, only an electrical systems engineer may work on a plant computer network of a nuclear plant. This is stipulated in the nuclear licence to operate
- IIoT require low latency communications and IP based communications are often not concerned with real time communications as retry or best-effort protocols are adequate for their needs. While this is fine on a corporate network, this could have far reaching complications for safety and reliability if a system 'times out'.
- Digital twins refer to vendor and OT organisation that have immersed IoT so that monitoring systems are feeding back real-time information to the vendor who is then able to model and refine the model over time having ability to first optimise performance and reliability and over time have predictive abilities based on the data being collected. Third party access also creates new threat vectors.
- Many OT vendors are expanding into IT and offering integration and future proofing expertise [72].

In theory CIO's and engineering managers should start to realise that convergence is inevitable and determine how to support the environment as they are starting to implement IT-centric solutions from their vendors [72], [73]. There is still a lot of research and understanding to be gained by studying cyber-physical systems and the risks and opportunities associated with them as well as the requirements for implementation [54]. Training will need to happen on both ends i.e. OT engineers being upskilled in terms of their IT skills and IT specialists being upskilled in terms of OT skills. This may initially be a major hurdle to overcome as both ecosystems have run independently in the past and only interacted at points where their technology intersected. 4IR (fourth industrial revolution) is

now a hot topic in most industries with lots of investment happening in this segment with increasing focus on cloud based computing and storage. Figure 11 shows the various industrial revolutions from the late 1700s to present, mapped to their complexity. Various bodies like ATREMIS and EIoT-A, are looking at reference models that merge embedded technologies with SOA (service oriented architecture) to enable interoperability and security when traversing these technologies [54]. This is still some way off and may for now just be 'Industrial *intranet* of things' until stable models and testing have been validated, but the potential for business optimisation and monitoring is already evident.

Leadership from engineering and IT need to collaborate and develop sound operating models to ensure a smooth transition into the digitalisation of operational assets. Implementing IIoT will increase in monitoring information and open up further avenues into remote management while exposing OT assets to associated security risks. These risks need to be quantified and effective controls implemented based on a graded approach, as is the case for reliability and safety in engineering environments. It is possible that during the initial phases of digitilisation, there would have to be very close interaction with IT-centric OT vendors until the organisation is at a maturity level to support themselves.

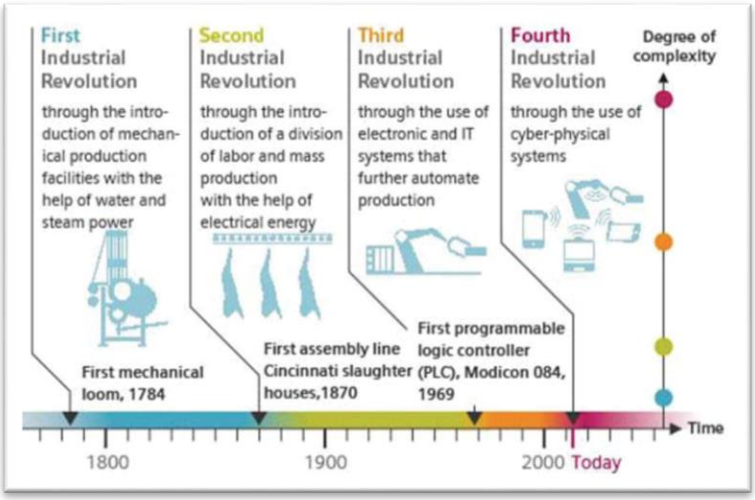


Figure 11: 4th Industrial Revolution [26]

IT-OT convergence and the implied use of common protocols, hardware, software and networking, may be a significant motivator for integrated security planning, incident response and recovery. A recent resilience exercise conducted by sustainability at Eskom, highlighted the erratic response to a potential cyber-attack in the OT environment. There may be efficiencies to be gained by integrating response functions and not splitting them especially if IIoT is adopted. Gartner recommends existing security governance teams have representation from both IT and OT represented with a consolidated SOC managing both corporate and engineering networks [74]. This may not be feasible in all organisations due to size and complexity but definitely aspects of this can be implemented for example a divisional IT and OT SOC, integrating both IT and OT cybersecurity monitoring tools. IT protocols are based on best effort examples would be CSMA/CD (carrier sense, multiple access/collision detect) that rely on retries to communicate between devices and applications. OT environments require low-latency deterministic communications and have their own standards and protocols that support this often measured in real time milliseconds with synchronised clocks. Another important concept is resilience which involves fail safe design practice, similar to redundancy in IT, but with engineering, there usually is no coming back from a failure as the consequences may be physical e.g. a chemical spill [73]. IT may need to update standards to address this once the demand for such is justified. This is currently being addressed by the IEEE and the IETF

to look at functionality like TSN (time sensitive networking) and standards dealing with the transport layer [72].

As IT moves closer to the physical world, an incorrect setting on a field device like a sensor linked actuator malfunctioning can have far reaching consequences like an environmental spill, explosions leading to injury etc. It is this reality that needs to be embraced by IT, that not everything can be reset or restored from a DRP backup [73]. IT GRC are very often led by finance or legal departments, this reality may not be fully comprehended and be seen as trivial [54]. OT follows a distributed model and in most instances IT is a centralised model, this means that cybersecurity decisions related to operational environments are made on the site or at group level (coal, nuclear, peaking) but with each site still having full autonomy over their plant and their protection systems. This non-standardised approach to cybersecurity does not enable the securely provision function of NERC-CIP as it is not uniform in its very nature. This has a cascading impact on resources, as they are not flexible to service the business in different environments, as they will need years to learn a system and these differ in different environments. It may be prudent to integrate robust engineering design principles into IoT and converged technologies to shorten the learning curve and produce solutions that do not compromise safety, availability and reliability [73]. It will be incredibly difficult to be fully converged unless the culture on both sides are the same and this can only happen over time and when both industries understand the requirements of each other, their mandates, roles and responsibilities, functions, interface points are clearly defined and meaningful metric introduced to measure performance of these.

2.6 Cybersecurity Maturity Models and Frameworks

The focus of this research is not on the maturity models themselves, but rather a sub-aspect of cybersecurity culture. The objectives of having a QMS (quality management system) is to introduce standardisation of processes, commonly trivialised by 'document what you do and do what you document'. Eskom is certified ISO 9001:2005 and currently moving to 2015. Continuous improvement is part of the PDCA (Plan Do Check Act) and requires us to continually evaluate what we are doing against established processes in the form of self-assessments and audits, which form part of our governance regime. With cybersecurity, many standards authorities provide frameworks like NIST, IEC, ISO, EPRI, NERC, and IEEE that can provide guidance for the implementation of cybersecurity in an organisation [8], [53], [62], [75]. Using a maturity model helps to measure the ability of an organisation to protect its assets from attack and its ability to minimise disruption [76]. Some other European standards from ENISA [41] identify the gaps and derive mitigation measures from the existing technical standards (e.g. ISO27001, ISO27002, BS 15000, EN ISO27799, PAS, PCI-DSS, COBIT, ITIL, BSI IT-Grundschutz).

Once an organisation has gone through the process of implementing a framework, the organisation is obliged to evaluate on the effectiveness of the implementation both from a general ISO 9001 standpoint and ISO 27000 series. Leading from this, most frameworks will have a maturity model and framework against which you can assess your implementation or existing cybersecurity strategy. This means is that one can use a maturity model to see how mature the Cybersecurity implementation and acceptance of the implementation is in the organisation. An example of a cybersecurity model is the C2M2 (cybersecurity capability maturity) model and it can be used to support for example the NIST framework [62], [17], [47], [54]. Most organisations choose a standard approach to IT governance and use this to measure compliance. Popular standards in use are the ISO 27000 series relating to information security, but which has obvious shortcomings, as the technical controls do not adequately address ICS. A newer standard PAS 555:2013 emphasises that technical measures alone are not sufficient; effective outcomes encompass people, behaviours,

physical equipment security, governance, leadership and culture. PAS 555 defines the fundamental outcomes that specific security practice should achieve, rather than how to implement them, understanding that the appropriate measures are likely to change rapidly over time. Whilst the standard recognises the need to specifically address ICS vulnerabilities in building control systems, industrial process control and manufacturing, it does not reference guidance for ICS security implementation [54]. NIST has a framework for improving critical infrastructure cybersecurity. It is outcome focused and technology agnostic and has been adopted as a standard against which Eskom measures cybersecurity maturity [13]. IEC 62443 are based on ISA-99 technical reports and focus on cybersecurity of industrial automation and control systems. It quite clearly differentiates between IT and automation and controls systems and corporate systems. There has been a drive by the coal power stations and their vendors to be assessed against this framework. Another framework that has a security focus is the Systems Security CMM, which is used to evaluate security-engineering processes and is standardised as ISO/IEC 21827, however it is not overtly cybersecurity focused.

2.7 Legislative Environment

Europe and America have many organisations responsible for developing strategies, frameworks, standards, best practice and regulations supporting rigorous cybersecurity protection. South Africa does not feature highly in the global political landscape to enable us to have such high standards for cybersecurity. We do our best to adopt international best practice and many of the sectors that require strong cybersecurity protection utilise consultants and/or adopt best practice from international sources. We did a scan on SABINET for approved cybersecurity legislation and could not come up with any acts or regulations, mostly bills that were still under review are published on their site.

National Cybersecurity Policy Framework:

The State Security Agency (SSA) is responsible for the National Cybersecurity Policy Framework (NCPF) which was accepted by Cabinet in 2012 and acknowledges the Information and Communications Technologies (ICT) as critical to economic growth and education [77]. The dependence of society on cyberspace has exposed users to cybersecurity threat levels never before experienced and priority is given to critical information infrastructure protection. The Policy framework aims to create a secure dependable cyber environment, increase cybersecurity awareness in South Africa while supporting security imperatives and economic growth. This calls for a tripartite alliance between government, the private sector and civil society to ensure that cyber-risks are understood and addressed at all levels. The NCPF will endeavour to centralise the coordination of cybersecurity activities by facilitating the establishment of structures, policy frameworks and strategies to combat cybercrime, as well stimulating the link between policy, legislation, societal acceptance and technology. It is also promoting international cooperation as well as compliance with technical and operational cybersecurity standards, developing skills and research and most notably relating to this research, promoting a culture of cybersecurity in order to comply with minimum security standards. Critical to these objectives is the formation of a cybersecurity response committee to coordinate cybersecurity activities, which in terms of NERC and NIST standards are fully aligned. This committee has the unenviable task of improving cybersecurity measures; intelligence collection and improved capacity to investigate, prosecute and combat cybercrime, cyber terrorism, cyber espionage, cyber warfare and other cyber related threats. Also related to this research, they will promote and provide guidance on the protection of national critical information infrastructure. The cybersecurity centre will focus on operational coordination of incident response activities, provide guidance to and facilitate the identification, protection and securing of national critical information infrastructure (NCII), by performing regular assessments

including vulnerability assessments. In short, a cybersecurity culture, driven in main by the State, is critical to ensure that citizens take advantage of the information age, whilst remaining conscious of the threats and vulnerabilities of cyberspace. There is a need to balance the risks associated with the use of information systems and the indispensability of access to information and communication via technology to the functioning of open and modern societies. The growing threats to Cybersecurity should not hinder the crucial role of information and communications technology in stimulating the growth of economies and society. To effectively deal with Cybersecurity, it is prudent that civil society, government and the private sector play their part in ensuring South Africa has a culture of Cybersecurity. Critical to this is the development of a culture of Cybersecurity, in which role players understand the risks of exploring in cyberspace. To facilitate the building of a Cybersecurity culture, the NCPF provides for inter alia:

- Implementing Cybersecurity awareness programs for private sector, public sector and civil society users;
- Encouraging business to develop a positive culture for Cybersecurity;
- Supporting outreach to civil society, children and individual users;
- Promoting a comprehensive national awareness program and guidelines;
- Reviewing and updating existing privacy regime;
- Develop awareness of cyber-risks and available solutions;
- Continuously review cyber applications and the impact from a Cybersecurity perspective;
- Complement the culture of Cybersecurity with online support mechanisms [16].

General Data Protection Regulation (GDPR)

While the GDPR was originally developed for the European Union, it is fast being adopted throughout the world [78]. The regulation serves to protect the rights of personal data held by companies by ensuring their privacy and protection. It also gives regulators rights to ask companies to prove how they protect data subjects' privacy. The financial sector in South Africa has been forced to architect solutions that comply with GDPR legislation. While there is no explicit mention of cybersecurity culture in the regulation, it is considered a critical resource in the realms of information security and hence worth a mention [79]. This has far-reaching consequences when dealing with information of foreign nationals on South African systems. Article 5 of the GDPR guides how personal data is handled and has seven principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability [78]. In 2018, it was agreed in the European Union that the GDPR would protect all EU citizens' personal data and all member nations would need to comply. It is important to note that any company that markets goods or services to EU citizens is also subject to this regulation regardless of their base of operation making it of global significance [80].

Protection of Personal Information Act 2013 (POPIA)

The Department of Justice in South Africa promulgated the above Act in 2013 that ensures the protection of South African's personal information. While this does not really apply to the OT environment as the data that needs protection is mostly machine data, control signals, sensor input and so on, there is the element of user credentials that may be considered personal information. However, our corporate network and business network have customer information residing in

various repositories that support the distribution and sale of electricity. The act serves the purpose of minimising financial fraud, identity theft, protection of privacy, which is a fundamental human right and is the South African equivalent of the GDPR [81]. Enforcement of compliance to the Act has started from July 2020 while the regulations was published in 2018 [82]. All South African institutions are compelled to conduct themselves in a responsible manner when collecting, storing and sharing the personal information of their clients and this Act can hold them accountable for mismanagement of this sensitive information.

Cybercrimes Bill

The Bill serves to create legislation that will criminalise the unlawful distribution of data, provide for protection orders and impose penalties on those who commit cybercrime. It was originally called the Cybercrimes and Cybersecurity Bill in 2017. In 2019 it was advertised for public participation and finally passed at the National Council of Provinces (NCOP) in July 2020 [83]. It further describes matters of jurisdiction, investigation, reporting and establishment of structures to promote cybersecurity as well as capacity building. It also regulates the identification and declaration of critical information infrastructure (which is different to the old national key point act) and gives the department of justice powers to interact with foreign states to protect South Africa against the perpetration of cybercrime. Cybercrime covers unauthorised access, illegal acquisition of data, cyber fraud, cyber-extortion and extends to malicious communication that incites violence, property damage, 'slut-shaming' by unauthorised distribution of personal images and videos, and so on. While the bill is focused on cybercrime and punitive measures, it does not explicitly mention cybersecurity culture but mentions capacity building and does not extend to national critical infrastructure like the ports but limits itself to information critical infrastructure like datacentres [15]. It is important to know the intent of this as it is the legislation against which any cybercrime in SA will be referred to and has the punitive power to impose appropriate punishment locally and internationally by leveraging of international agreements as cybercrime is not limited to national borders [84].

Critical Infrastructure Protection Act 8 of 2019

The Critical Infrastructure Protection Act replaces the National Key Points Act of 1980 [85]. The aim is to identify and declare all critical infrastructure in the country and provide for measures to be put in place to protect and safeguard including resilience planning. Eskom's generation sites, transmission lines, distribution networks, national control centres are all considered critical infrastructure and as such need to have robust processes in place to protect from physical and cyber threats [3]. There are provisions for a council that will effect the mandate of the Act. Eskom has a role to play in resilience response even when other related critical infrastructure are affected and have various representatives at joint operations centres [16]. The Act also provides consideration for what infrastructure is deemed critical and from the definition, Eskom is considered critical to the stability of the country. It also makes provision for a council who will consider and make recommendations in respect of applications and report to the Minister of Police [86]. The regulations are currently in the process of being drafted.

2.8 Summary

The literature review has highlighted aspects of cybersecurity, culture, leadership, organisational influences, group dynamics, as well as environmental challenges common to utility environments. There are many dimensions related to culture and include (not exhaustively): attitude, behaviour, compliance, responsibility, accountability, self-efficacy, commitment, reporting, communication,

trust, ethics/ values, collaboration, knowledge, norms, perception/assumptions, cognition and vigilance. These insights are used in the following Chapter to design and implement the measurement instrument for culture baseline establishment. This Chapter has also described the differences in IT and OT security as well as the challenges of convergence and the impact this may have on the behaviour of staff. Maturity frameworks was also visited, as culture, training and awareness form part of the frameworks. We have also noted that the level of culture integration is dependent on the risk profile of the organisation.

3 Methodology

The intention of this study is to obtain a dipstick assessment of the cybersecurity culture in Eskom in order to develop a business case for a cybersecurity culture program. Various methods are used in the references quoted in Chapter 2 ranging from focused interviews, simulations, metrics to questionnaires with the latter being the most popular. When developing a business case for the implementation of a cybersecurity program, one needs to establish a baseline and identify the gaps that exist between your current and target state and the initiatives that will help make the transition. Aside from questionnaires and interviews, results from simulations and sector based statistics can also be used to support the program [33].

An organisation wide view of the cybersecurity culture was needed in a short frame of time as project budgets needed to be submitted by January 2020. The CoE has designed and presented a cybersecurity fundamentals course for OT staff that is ECSA accredited for CPD. To date over 200 people have been trained but we found that only those who know about the course are being trained, as it was a very focused campaign. Classes are small, instructor led, with attendees at various levels of cybersecurity maturity. We have no measurable way of determining how it has impacted the overall OT environment. Already having this focused approach, it made sense to employ a more generic approach but focussing on the OT environment, to measure culture. Because we do not do these organisation wide assessments all the time (as it creates fatigue and non-responsiveness), we needed to design an assessment that was broad enough to cater to the entire organisation but at the same time being able to extract the information we need using analytics. The broader results obtained can further be analysed for example by the information security team. We opted for a questionnaire, which met these criteria quite well, however going forward we will use a combination of the prior mentioned avenues to implement and evaluate effectiveness of implementation.

3.1 Tool Selection and design

Chapter 2 references multiple behaviour models, like the KAB (knowledge attitudes and behaviours model), behaviour modification theory and protection motivation theory;- these primarily focus on the cybersecurity culture of the individual [38], [11]. Each of the models have significant overlap with a bias to some of the elements but they mostly align to the KAB with cognition, communication, compliance, norms/beliefs/values and responsibilities as further measures. Individual to individual interaction can be different in a group setting and some studies acknowledge the role of groups and inter-group relations and the impact this has on cybersecurity- essentially with the right stimulus groups can form their own cybersecurity culture [6].

Some other studies also acknowledge that leadership play a strong part in driving cultural transformation and a few of the cybersecurity studies also incorporate elements of leadership and their role in driving strategy and transformation initiatives [17], [87], [64].

Humans also interact with technology and organisational processes that further contribute to added cybersecurity protection in a layered manner also referred to as defence in depth. Many of the process and technological controls are also configured or developed by humans and consequently are potential sources of vulnerability, after all a firewall is only as good as the configuration of the rules set on it.

Cybersecurity culture is largely considered a subset of organisational culture and consequently a view of how the organisation embraces cybersecurity culture is very important [88]. Often, organisational culture initiatives focus on high level strategic objectives with cybersecurity not

overtly being included. Support at organisational level is essential to delivery of cybersecurity culture transformation and results from the questionnaire will be used to canvas the support of the organisation at executive and Board level.

Cognition and group dynamics as described in Chapter 2 highlight the impact of culture in small groups because of the effect of imitation, instruction and collaboration, and while this may be so, it was omitted as a major category but elements of group dynamics was captured in some questions [6], [89]. The reason for omission is that the level to which we drilled down to in the demographics was not at group level as Eskom has a national footprint. Group constructs will be used at the implementation stage by using pilot sites for testing initiatives; this is also the approach utilised by other culture initiatives in Eskom. At a leadership level there are three main measures of cybersecurity namely priority, participation and knowledge [6]. At a group level, dimensions of norms, shared values and commitments gain focus. Knowledge is very closely linked to self-efficacy, and behaviour change is optimal when cybersecurity is part of work processes, leadership commitment for cybersecurity is tangible and proactive and if it supports organisational strategy, goals and objectives. It is important also that cybersecurity does not place an additional burden on individuals related to production or department objectives, as most employees would choose to meet their performance objectives [11], [39]. Communication, trust, collaboration and integration of cybersecurity into business processes are also positive artefacts of culture. As culture transformation matures, it will start to foster security awareness in the organisation and heightened risk perception and a sensitivity towards changes in threats [50], [51]. This does not paralyse an organisation but rather promotes risk informed decision making [17].

In parallel to the literature review conducted, we also investigated how safety culture transformation was being achieved in Eskom and looked at similar programmes in the nuclear safety culture environment at Eskom. My experience in the nuclear sector and exposure to nuclear safety culture transformation and the broader teams exposure to safety culture translates to familiarity with the tools and methods used to measure and transform culture. Nuclear safety culture was introduced around 2008 at Koeberg Nuclear Power Station and it took at least 5 years before the broader organisation started to adopt a similar approach. The corporate safety culture department has made great strides in transforming culture and we have much to learn and collaborate on, as the scale of a corporate initiative is far greater than that focused on a single power station. Corporate specialists focused on individuals, leadership, processes and organisation in their campaigns. We thought it would be a good idea to align to this approach, as it was more comprehensive than those used on most of the culture measurements we researched and found that it aligned to Schlienger's organisational model of 2006 and also to Schein's organizational or corporate culture theory from 1985 (referenced in 12 papers) [63]. Typically, most of the academic literature focus on information security and measurement of individual culture. Companies that sell cybersecurity transformation solutions focus on around seven dimensions viz. attitudes, behaviours, cognition, communication, compliance, norms and responsibilities. Additionally trust, perception, self-efficacy, ethics and values are also dimensions of interest.

The questionnaire was divided into four categories:

- Individual (including demographics)
    - Knowledge
    - Attitudes and perceptions
    - Behaviour
- Process and technology

- Leadership
- Organisation

These are the four main touch points of cybersecurity culture as it focuses on the areas in which we practice cybersecurity. Our task was to establish a baseline and while most academic studies focused on the individual and while it is extremely important, there is a broader perspective to be explored and ignoring the other three components would set the transformation project up for failure.

The dimensions that were tested for the four main categories were:

Attitude	Behaviour	Knowledge
Compliance	Communication	Norms
Responsibility/Accountability	Trust	Perception/Assumptions
Self-Efficacy	Ethics/ Values	Cognition
Commitment	Collaboration	Vigilance
Reporting		

Table 2: Dimensions of culture that was measured

Attitude, behaviour and knowledge were evaluated as subcategories of the individual main category; however, elements of these also straddle the other categories. The colour coding in table 2 above shows the related dimensions as described in Chapter 2. Norms, ethics, values and collaboration relate to group dynamics traditionally. However, collaboration, trust and cognition are also closely linked. In simple terms, cognition refers to the mental process of gaining knowledge and comprehension of which there are eight cognitive capacities. The questions were first evaluated at the CoE, then further sessions were conducted with the nuclear safety lead as well as their external psychometric consultants. We then involved the enterprise risk and resilience and organisational design to review before piloting the questionnaire.

Analysis was done on a sample audience as Eskom has over 40000 employees, and it was not an easy task to access just OT and IT staff specifically. The minimum number of respondents was determined to be 381 using a validated statistical formula for sample size calculation (see Chapter 4). We originally intended to target only OT staff, but due to time pressures and the difficulty of getting a comprehensive list of purely OT staff, we had to ensure that the questionnaire could be circulated to the entire organisation but with the ability to distinguish between different groups and filter out the relevant observations. The hypothesis was that IT staff have a more mature cybersecurity culture and we intended using them as a benchmark initially, to observe their strengths and later look at synergies in strengthening culture in OT. With the presentation of the new cybersecurity operating model, this may be reality as there is a consideration of merging IT and OT cybersecurity Centre's of excellence under combined leadership at executive level.

Objectives of questions

According to ENISA, there is low correlation between demographics and cybersecurity culture, however demographics was captured to be able to target interventions per division or function [11]. The intent of the questions is captured below and is not exhaustive but describes the types of questions that was generated.

- Knowledge based questions focused on whether respondents had undergone training, their background and skills related to IT and OT, if they read awareness messages, practice secure design and efficacy related to recognizing social engineering attacks. We also include some specific OT control questions to test if perceived knowledge is valid.
- Attitude questions also included perceptions and addressed willingness to learn, pain points like password changing, organizational vulnerability to cyber-attack, sharing of cybersecurity knowledge, teamwork, interdependency, responsibility and trust
- Behaviour also relates to sharing of insight, how users behave with removable storage, their personal cybersecurity habits, reporting, trust and compliance, ethics, response
- Leadership was largely perception based and we looked at how managers react to incidents, support, responsibility, budgeting, commitment and priority, risk assessments. Depending on the responses from managerial level, one could also gain insight from their observations
- For process and technology, we investigated reporting channels; effectiveness of controls, security management, perception of efficacy, business processes that support cybersecurity, impact on other objectives and innovation, access control. This presents an opportunity to gain insight into dependence on technology in OT as well
- Organisational questions explored aspects like; accountability, compliance, budgeting, organizational culture, trust, values and commitment (these last three are also related to group dynamics).

3.2 Questionnaire Execution

Based on the above we created 49 questions with seven of these related to demographics. Likert scales are widely used in questionnaires and is a unidimensional scale that is used to capture attitudes and opinions [90], [91], [92]. An Odd Likert 5 point scale was used with a range from strongly disagree to strongly agree introducing a neutral option between extreme responses. In some instances we also had a 'not applicable' (where questions where specific to group or discipline), very low to very high and normal numeric from 1 to 5. Some questions had specific types; an example is choosing attack vectors which helped show frequency distribution and uncertainty. It was crafted using previous questionnaires with similar factors and dimensions that were identified and validated in previous studies and now tested for reliability. This is shown in Appendix 8.3 where the four main categories or factors were defined and also showing the thirteen dimensions or sub-factors as identified in previous studies [65], [63], [43], [11], [33], [41]. The factors and sub-factors vary greatly across studies and it is essential to contextualize for the environment tested, which was done in this study. The use of multiple Likert scales for optimum readability however created an additional complication of data cleanup, which in this case was very substantial as all the different scales and questions had to eventually range between a 1 and 5. Branching logic was executed on a few questions, for example; where we needed to drill down into demographics and the questions were eventually completely randomized with the identities of respondents kept anonymous. The questionnaire was also piloted with a limited audience of 5 people to ensure that it was valid and functioning correctly and feedback incorporated into the final questionnaire.

The questions shown in appendix 8.3 as a table were designed using principles for questionnaire design by making them neutral, non-leading and unambiguous and favouring a Likert. The last column in the table describes the scales used per question. Some of the choices are multi-selection with the intention of identifying convergence or divergence and was introduced where we knew there was a lack of clarity. This also enabled the analysis to ascertain relative importance of the choices selected. Reliability and consistency calculations are generated using the categories column

in the table. Once the design and tool was selected, it was deployed on an internal SharePoint platform, keeping the identity of respondents anonymous. Using SharePoint also ensured easy integration to Excel and Power BI applications. At the end of the one month period that it was open, the questionnaire was closed, exported and subsequently archived. 413 responses were received from various departments in Eskom.

4 Results and Analysis

SharePoint has a built-in functionality to automatically display the results from a questionnaire as received. It is fairly good and one can easily get an initial 'feel' for the data, but it is not detailed enough to provide the insights needed for indepth analysis. With this in mind a process was formulated to process the information, bearing in mind that the questions would need to be eventually linked back to the main categories and subcategories and show relationships between these where possible with numeric scoring to give the organisation a picture of how it is performing with respect to cybersecurity culture. Thereafter analysis was performed per category and across categories to describe the story that the data was obfuscating. Due to the nature of the questionnaire and data types (ordinal), descriptive statistics was used in a limited manner and a data science approach chosen over this because of the powerful dynamic way data is analysed and the relationships that can be highlighted that are not immediately evident from numerical statistics. Traditionally bar charts are mostly used for displaying of questionnaire results as the actual frequency of distribution often presents a clearer picture than summary statistics [93] .

4.1 Data Processing

As alluded to earlier a process was formulated to process the data to be able to analysed. Figure 12 below shows the high-level activities that were identified and performed on the information in the various applications used. Each of these applications while having similarities, had some distinct advantages for certain operations.

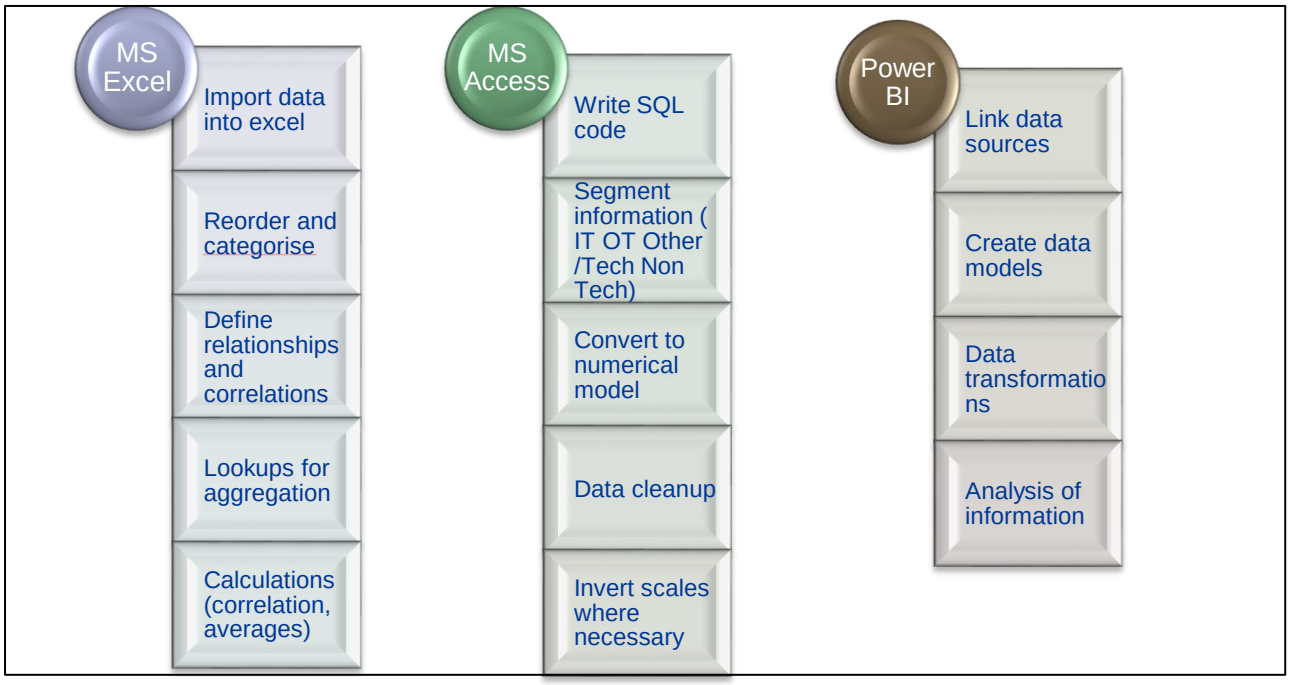


Figure 12: Data manipulation process

Initially a live link was created between SharePoint and Power BI but once the questionnaire had been closed, a data dump was done and imported into Excel. Power BI requires a data model to be defined and the data directly from SharePoint was not suitable for analysis to be performed. Once the constraints were defined, the data was firstly reordered and categorized as it was originally designed as the data had been randomized in SharePoint deliberately. This was done by creating numbering systems between the original and exported files, which was different to the intermediate reviewed file as the branching logic, and multi-choice questions had created additional fields that

needed to be rationalised and updated as well as correlation numbers inputted. It was also helpful to have the categories colour coded for visual quality checks. All data manipulation in terms of ID's, switches, lookups and calculation fields done was then performed in Excel. All of the standard 'strongly disagree' to 'strongly agree' was then immediately converted to a numeric 1 to 5 scale. For others that had modified Likert versions, conversion look up tables were created to aggregate back to the standard 1 to 5. Some of the questions were phrased in a neutral or reader friendly way and when converted to a Likert scale had to be reordered or inverted. These questions are marked with a yellow asterisk symbol on the graphics. At a later stage, it was found that the process had not completely converted the descriptive Likert to numeric Likert, a further validation was done by confirming that the average of the field was numeric. Pearson correlation co-efficients was also calculated in Excel due to the ease of use of formulas as opposed to Power BI which was good at showing this correlation graphically. This showed the level of correlation between questions and vary between -1 and 1. A value of zero indicates no relationship [94].

This excel sheet (owssvr.xlsx) was then linked in MS Access. At this point, it was necessary to create a column for IDs as user IDs were hashed when 'anonymous questionnaire' was selected when designing the questionnaire in SharePoint. The subsequent step required the data to be comprehensively separated into IT, OT and the rest of the organisation and subsequently technical vs non-technical people, which will only be used at a later stage when designing interventions across all areas. A set of criteria was developed to separate the data as there are OT people with IT experience and some IT people with OT experience. We also linked their responses to department type and demographics in terms of whether they were part of business or Group IT. The actual SQL queries are captured in the appendix of this report. The functions below represent the factors as used to design the update queries

OT = f(OT_background OR IT_Background AND dept_type{Eng OR OT})

IT = f(IT_background AND Group{IT} AND OT_Background{No})

The conversion to numeric was also done in Access using the replace function using a phased approach. Eventually even multi-choice questions were also converted to full numeric format, however this was only done after all analysis was complete and summary scores were being generated (Mastnum) of the excel file. At this point errors in the data clean up were also highlighted as certain fields were not able to calculate summary statistics. The data was exported out of MS Access back into Excel for its ease of use for statistical calculations and formulas. Some of the responses had to be inverted so that one is consistently a low or 'unpreferred' response and five a high or preferred response. Parallel tables were created for visualisation and for calculations. Once the summary statistics was verified, this dataset was then re-imported into access to enable a connection into Power BI (NewMastNum). If this questionnaire was to be used as an industry standard for example, one would use Cronbach's alpha co-efficient to test for reliability and the 'NewMastNum' table is in a suitable format to be assessed. However, when creating a framework or de facto industry standard, you would need to have the results obtained across a variety of populations tested against each other to be able to calculate its reliability. In this instance, our interest is purely internal.

The Access database file (Culturedatabase.accdb) was used as the source of the data analysed and a connection was created to it from Power BI. All updates were performed either in the source excel file (NewMastNum.xlsx) or in the database for 'Mastnum' table. Once the link was created, the data model had to be configured and the relationships established between the various tables. The tables were created according to the categories described in section 3.2. Lookups were created in

MastNum and was linked to the data model; however, Power BI had some issues resolving the lookups which resulted in a lot of extra work and circular references. The lookups were supposed to be used for ordering and ranking of the data, but did not work correctly and was eventually solved at the database level. The transformation functions in Power BI was used to create sub tables from the master table for each category and subcategories were necessary (shown in the Appendix) and these extracted only the fields related to a category. Power BI also uses a built in scripting language called DEX which was used to perform field calculations where needed. Eventually four different Power BI files were created due to the memory intensive nature of the application and the number of relationships and graphics needed per category. Graphics was generated per question and mostly differentiated between IT and OT across questions. Power BI is very powerful for analysis as it can be set up to dynamically filter across all reports or only a single one, it can also either filter or drill up or down depending on how data is configured, and you can look at the relationship between any question by dragging in that graphic onto the report you are busy with. Bins as used in statistics is easily generated either using DEX or existing fields in the data model but with better ease of use and dynamically relating to whatever data you have displayed on a report. The data clean-up was an ever-evolving process until all the anomalies were resolved. This enabled the data to be completely rolled up for summary scores should the enterprise want an actual score, the value of which could be debatable as it was done using median and averages both of which are not extremely accurate for descriptive statistics.

4.2 Data Analysis

The sample size was determined using a statistical formula shown below in figure 13 where N is the population size, e is the margin of error in decimal format and z is the z-score or the number of standard deviations a given proportion is away from the mean (obtained from a table) and p is the population proportion [95].

The input values for the formula are:

Confidence level (95%) this is the probability that the true value being studied falls within a range of specified values.
Margin of error (5%) also referred to as a confidence interval; it is the sampling error in a

$$\text{Sample size} = \frac{\frac{z^2 \times p\,(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p\,(1-p)}{e^2 N}\right)}$$

Figure 13: Formula for sample size calculations [93]

questionnaire.
Population proportion (50%) is the percentage of a value associated with a questionnaire in other words we are saying that 50% of the population work in OT.
Population size was inputted as 43000.

Using the above numbers, the sample size was calculated and independently verified at 381 responses using an alternative online sample size calculator with the same inputs. If one uses a population proportion of 30%, which is more realistic than the prebuilt 50% available in most online sample size calculators, the sample further reduces to 321. Three sites were used to calculate and verify viz. questionnairemonkey.com, calculator.net and qualtrics.com [95], [96], [97]. Upon closure of the questionnaire, 413 responses was received (see appendix 8.4 for images). Correlation where used in subsequent analysis is synonymous to 'infers' unless specifically calculated using a formula, where that will specifically refer to a correlation coeffiecient. Inferences were tested with the AB test and it is acknowledged inferences for a pattern or relationship are not unique and that a single factor could be one of many influencing a particular observation or outcome.

The questionnaire data was collated and results analysed and presented below. Some questions tested user attitude and was used to profile certain behaviour. An example of this would be: does the user have antivirus or antimalware on his phone. The behaviour exhibited can be used to infer employees' capacity for risk and in turn the possible exposure of the organisation to risk. The questions were developed in collaboration with the subject matter experts (SME's) in OT, behaviour based safety, nuclear safety culture and external psychometric experts specifically focusing on cybersecurity. Perception based questions for example those around awareness training and response to perceived risk, were used to evaluate effectiveness of cybersecurity culture initiatives. We can compare the measures to existing information security culture frameworks, but alignment to Eskom organisational culture is more critical and will be the focus of this study.

Internal consistency or reliability can be calculated using a number of techniques: average inter-item correlation, average item-total correlation, Cronbach's alpha, split half reliability and composite reliability. Some of the studies referenced in Chapter 2 used Cronbach's alpha [43], [65] to determine reliability of their questionnaires. A calculation was performed on our questionnaire using R and the psych library and produce an internal consistency of 86%, which is very good. We verified the result using a composite reliability calculation and this also yielded a value of 84% (see appendix 8.7) [98].

4.2.1 Demographics

Of the 413 respondents 44% was from OT, 43% was general staff (Other) and 13% IT. Distribution division had the highest response rate and correlates well to the conversations we had with their leadership and their commitment for staff to contribute, as their General Managers endorsed the

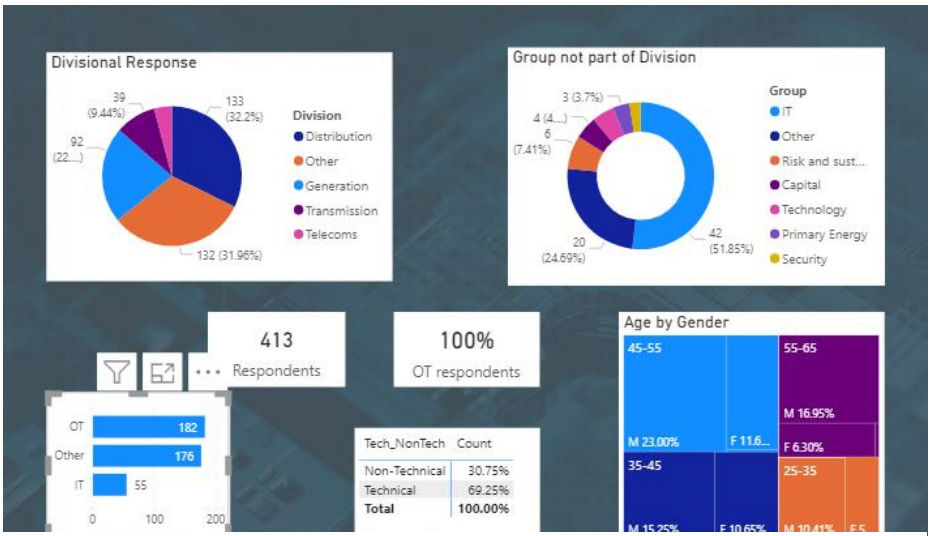


Figure 14: Demographic results

questionnaire and sanctioned the distribution to their OT staff. Other was in fact the largest contributor and comprised the smaller groups that did not form part of the big three divisions (Generation, Transmission, Distribution) as shown in figure 14. Other, when referring to Divisions, include the following groups: IT, Enterprise Risk and Sustainability, Capital, Technology, Primary Energy, Security and any other group that was left out. Interestingly the ratio of technical to non-technical people on the questionnaire was 69% to 31%, which means that most people who responded were not general administrative people, but people who had some engineering or IT background. It was interesting to note that in the OT space the number of male responses was significantly higher whereas in 'Other' the responses to the questionnaire was almost equal in the age group below 55. IT gender demographics showed some interesting observations with more females responding in the 25-35 category than males, equal in the 35 to 45 and 55 to 65 category, with 45-55 showing decidedly higher male responses. There was an even split between junior and senior staff members and only 2% of responses were from senior management.

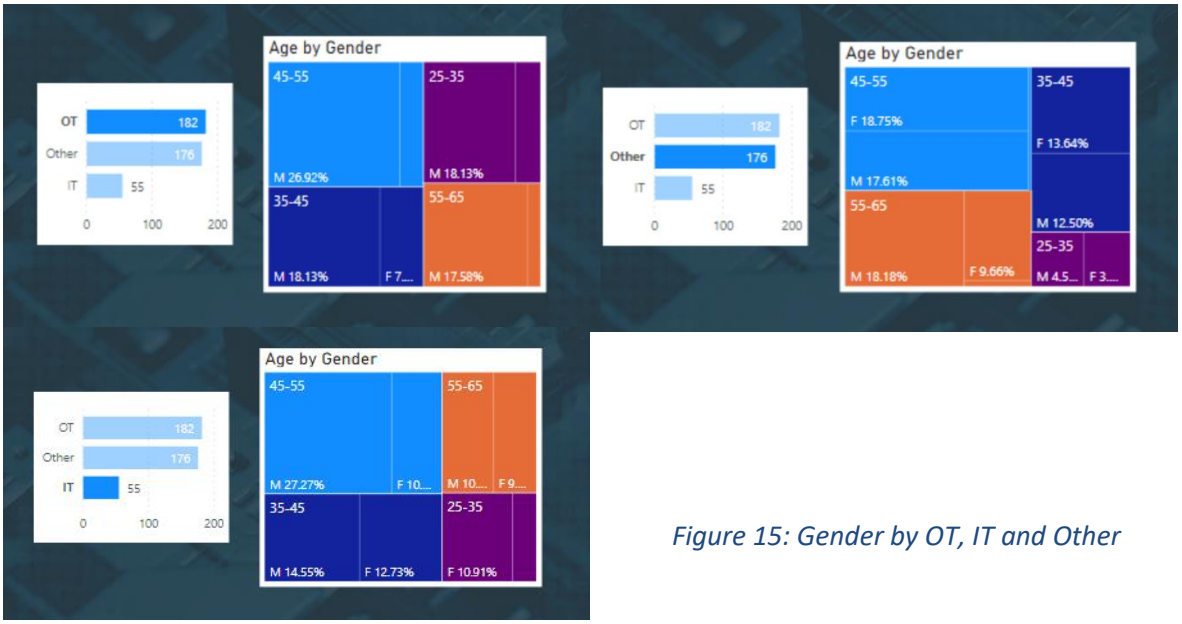


Figure 15: Gender by OT, IT and Other

4.2.2 Individual Knowledge

From a knowledge point of view, the majority of OT people have average to excellent cybersecurity knowledge and average to excellent computer skill, this is a favourable place to be. A similar spread is seen in IT as well. The SSC CoE (Security Solutions (Cyber) Centre of Excellence) had together with OT specialists developed a standard for OT cybersecurity and subsequently created a training team who rolled out classroom training on this standard to the OT environment.

Figure 16: Cybersecurity standard awareness

More than half the OT respondents are unaware of the OT cybersecurity standard and even more of them are also unaware of the training offered. This suggests that the method of communication for creating awareness of the standard is not very effective. Incidentally, these respondents are also largely eager to learn more as can be seen in figure 16. It is a challenge to spread awareness of the standard to the OT organisation as a comprehensive list of these resources are not available per business area. There is generally a more positive trend in IT towards learning than OT but they are still both positive. Training does show slight improvement on knowledge questions. Surprisingly training did not result in significant behaviour change yet.

Simple metrics like whether respondents recognize phishing attacks has been captured and the results from this can be compared to data we collect when we eventually do create simulated phishing attacks as part of the culture transformation program. The data collected for most of these singular type metrics will be used to monitor progress and efficacy of programs implemented.

We also found 37% of respondents who have a good computing aptitude as well as high levels of cybersecurity understanding are not involved in cybersecurity projects. These same respondents are also eager to learn (figure 17 below) where respondents in OT who are not involved in cybersecurity projects were selected. 'I practice cybersecurity in my work' was a control question and the high number of responses that practice cybersecurity while not being involved in projects suggest that there may be confusion with information security policy adherence vs cybersecurity. The information security awareness messages are visible throughout the business and create a sense of awareness around cybersecurity, but their focus is information security.

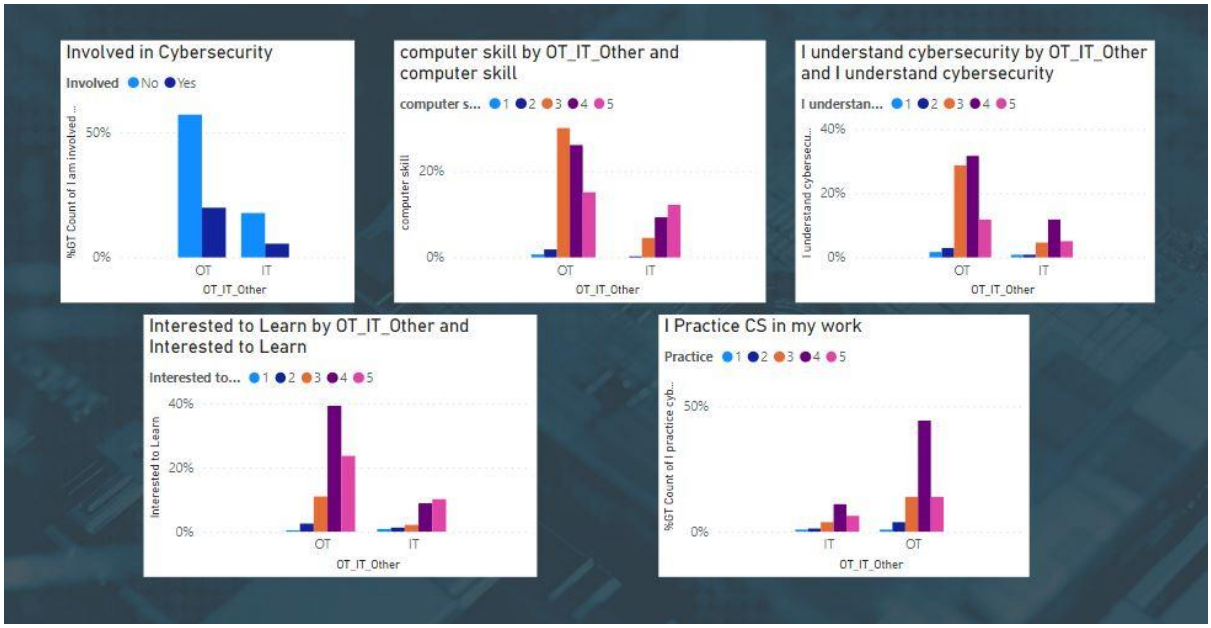


Figure 17: Not involved in cybersecurity projects with cybersecurity skills

We see a similar picture for people involved in cybersecurity projects in IT, but the results are not that surprising as IT has many processes and areas that they focus on like projects, service management, security, business enablement, solutions and so on. Everyone should have good computer and cybersecurity knowledge, but they mostly stay in the areas in which they are employed while drawing on their base IT knowledge. Attitude towards learning in IT is also more positive than in OT as well as levels of computer skill.

As part of a verification of respondent perception of their knowledge, a few questions of a technical nature were included. The results are shown in figure 18 and demonstrate that even though some people consider themselves to have very good to excellent knowledge; they did not choose the most

correct answer. The results are filtered by selecting only IT and OT staff who have very good to excellent knowledge (4 and 5s). This is also a trend picked up by other companies and research, that staff are overconfident in their knowledge and abilities [30]. This can be risky if the people configuring systems are overconfident in their own abilities, and supports that the protection technology affords, is only as good as its configuration, which is done by humans.

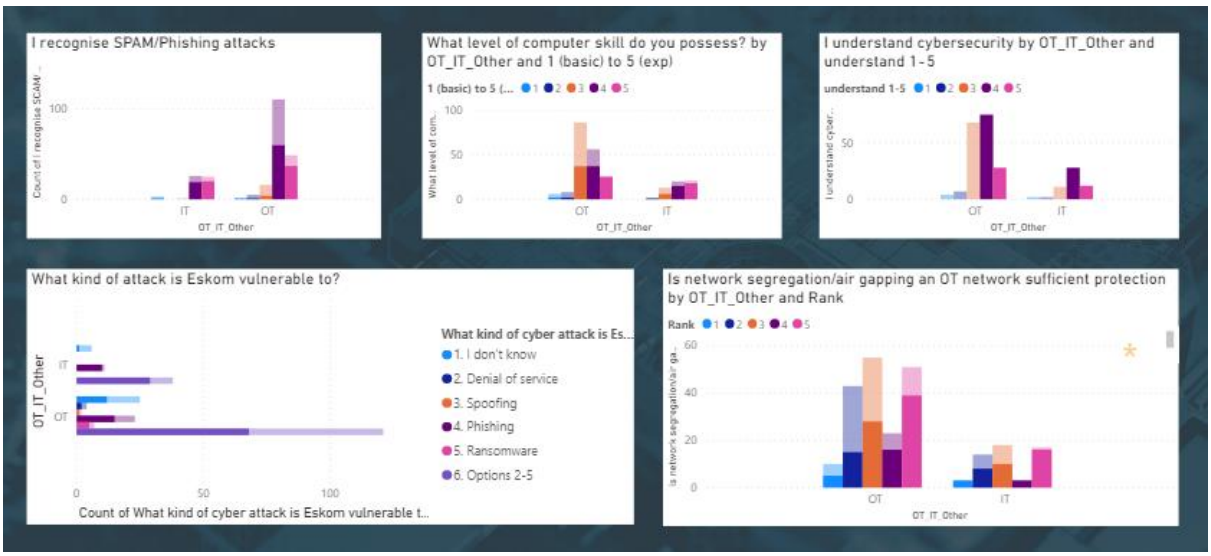


Figure 18: Technical knowledge of OT and IT staff

IT responses was generally better for attack vectors that Eskom is vulnerable to, however they also had a fair amount who chose less correct answers and from the network segregation and air gapping question it is apparent that both IT and OT do not have a good grasp of the concept and the protection levels it offers (discussed in further detail in section 4.2.7). Respondents rate their ability to recognize spam and phishing attacks as very good to excellent. Upon implementation of the cybersecurity culture transformation project this can be tested with simulation exercises, which once baselines have been created, more advanced type phishing attacks like spoofing attacks can be implemented.

4.2.3 Individual Attitude and Perceptions

42% of OT do not trust corporate personnel to work on their systems and 70% scored three and below. This is a double-edged sword as it is good to be wary of external people working on systems but from an internal trust relationship, this can be challenging.

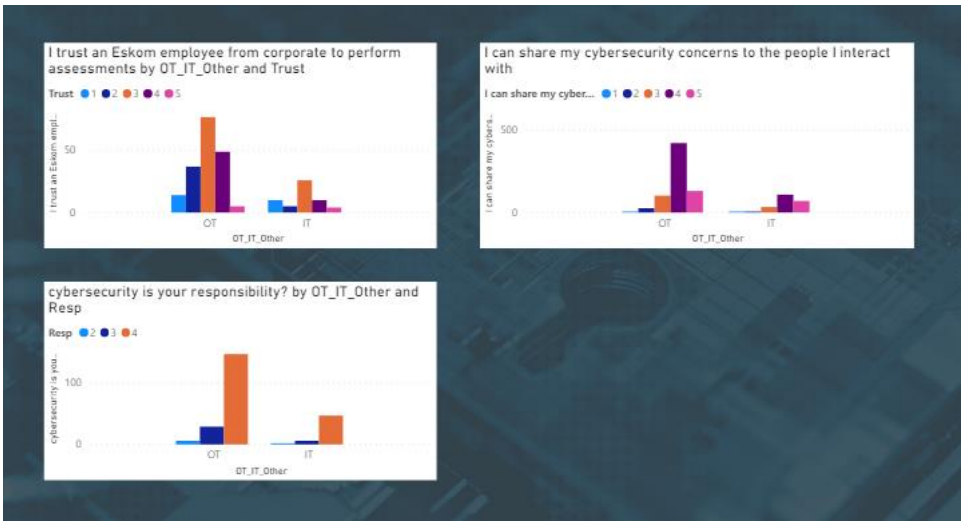


Figure 19: Trust, sharing on concerns and personal responsibility

With Eskom adopting a functional leader model, CoE's will have to build up trust and work closely with line functions to create alignment, value and adequate reporting as required by a corporate office. Sharing of cybersecurity concerns is largely positive as can be seen in figure 19, so the assumption that line functions want to hide their vulnerabilities from corporate functions to not expose weakness seems uncorrelated. It is more likely from our interactions that they are protective of their domains and this may be construed as a lack of trust. Overall, OT and IT take their responsibility for cybersecurity very seriously, and this could contribute as to why they do not trust corporate colleagues to work on their systems. A high level of personal responsibility can directly relate to accountability and ownership, and this can again result in distrust as objectives at an operating level can be at odds with those at a corporate level. An example of this could be operational cybersecurity versus ensuring compliance to corporate cybersecurity standards, which could be more high level and holistic in contrast to keeping a piece of equipment safe from cyber-attack.

Respondents show restraint when having to change passwords; however, there is still room for improvement on this measure. Access control is the first line of defense and its importance can be addressed by awareness messages on the importance of changing passwords. When selecting all the respondents that feel annoyance at changing passwords, they are spread across the entire spectrum from 1-5 for all the other measures in figure 20, so while there is a higher spread for annoyance it does not correlate to unsafe behaviour- there is no causality using AB method. The majority of staff would not choose to disable their antivirus and believe that cybersecurity contributes to safe plant operation. Staff in IT and OT largely believe that we are vulnerable to cyber-attack, but there is about 28% who are not convinced of this. Again, when analysing the data, there is no correlation to any of the other measures in figure 20.

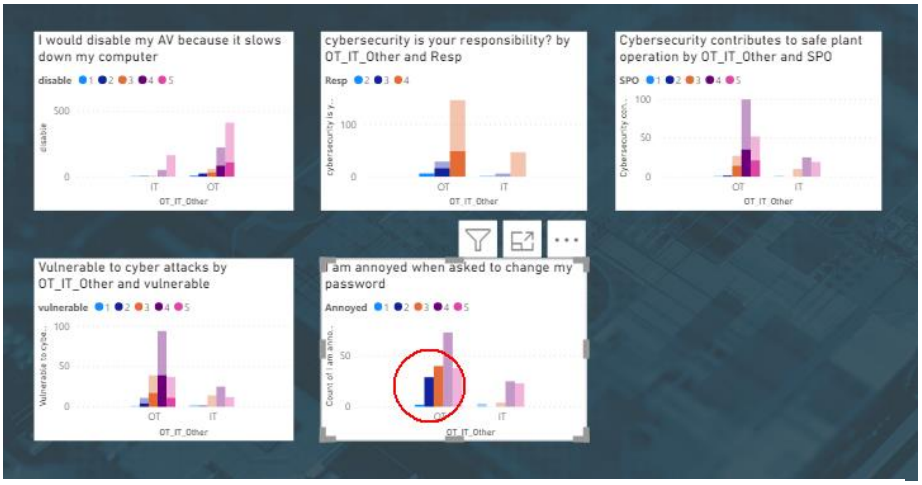


Figure 20: Safe plant operation, annoyance, disable antivirus

4.2.4 Individual Behaviour

Compliance to policy is important to staff mainly because they care about Eskom and they do not want the business to be impacted by a cyber-attack as seen in figure 21. This also ties in well with protection motivation theory that fear is not a good motivator for behaviour change and is in keeping with the organizational culture where staff who join usually stay for long periods of employment as compared to workers external to Eskom. There is a high sense of loyalty to Eskom and compliance due to being embarrassed, fearing consequences and valuing their jobs were significantly lower. This was also evident in the response rate as this was a multi-option question. There is moderate fear of consequences and value for their jobs again correlating well with organisational culture where most people are loyal and value their jobs as they see Eskom as an employer for the long term. Compliance is often not considered a measure of maturity by culture practitioners but it is a contributor to security culture.

Figure 21: Compliance to cybersecurity policy

Fifty one percent of OT staff scan removable media before using them while 67% do not report vulnerabilities As shown in figure 22. Scanning of USB devices reflects on how risk averse a user is and has an impact on the OT environment where networks are segregated and not usually connected to the internet, they also sometimes do not have the best patch management and this is a real attack vector in terms of insider threat. It is important that physical security also understand these kind of risks. Fifty five percent of OT staff have antivirus on the cellphones and while 75% read cybersecurity awareness messages (which is good), only 53% share their insight.

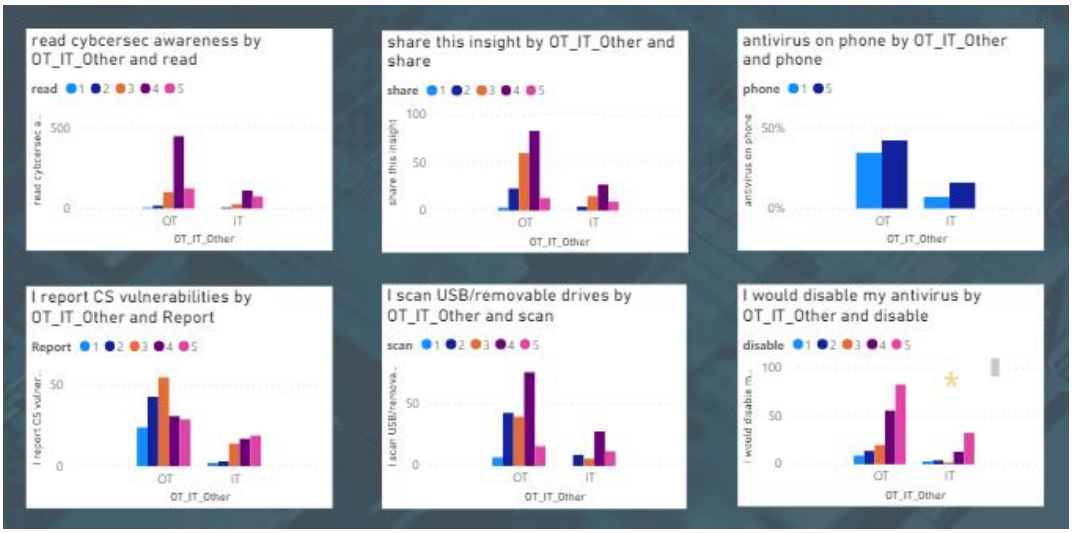


Figure 22: Sharing of insights and concerns

Having antivirus on their phones shows deliberation and acknowledgement of personal risk and proactive behaviour that may influence positive behaviour at work if we can relate it to them

personally. We specifically asked these questions to show maturity in behavior and links to group dynamics and interdependency where an individual moves on from looking after himself to looking out for others- one of the nuclear safety culture human performance tools/traits. There is average correlation between 'I can share my cybersecurity concerns to the people I interact with' (perception) to 'I share insights from information or messages I read' which is active behavior as seen in figure 23.

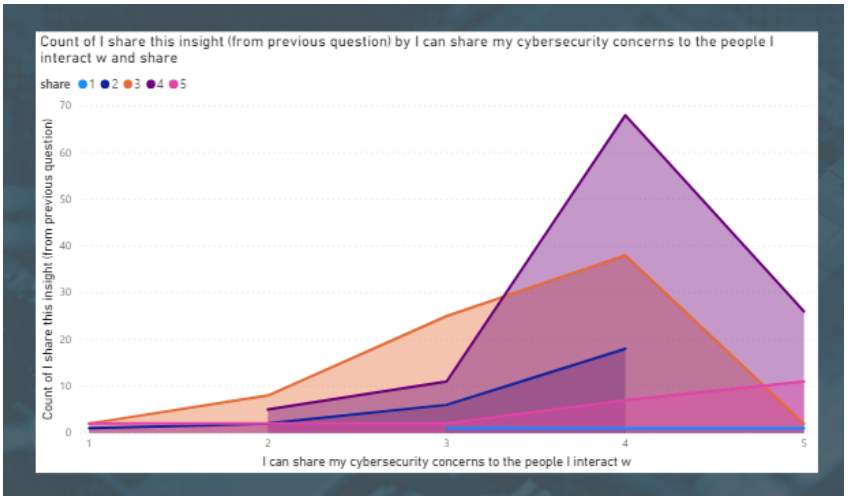


Figure 23: OT cybersecurity behaviour

The orange ideally should be more evenly spread between 1 and 3 but we can test for improvements on this measure in the next assessment. We have also previously mentioned that reporting of vulnerabilities in OT is not where it needs to be with 67% not reporting in contrast IT shows a much better trend. Figure 24 shows that even though respondents realise that they are responsible for cybersecurity and that it contributes to safe plant operation and that Eskom is vulnerable to cyberattack, people still choose to not report vulnerabilities.

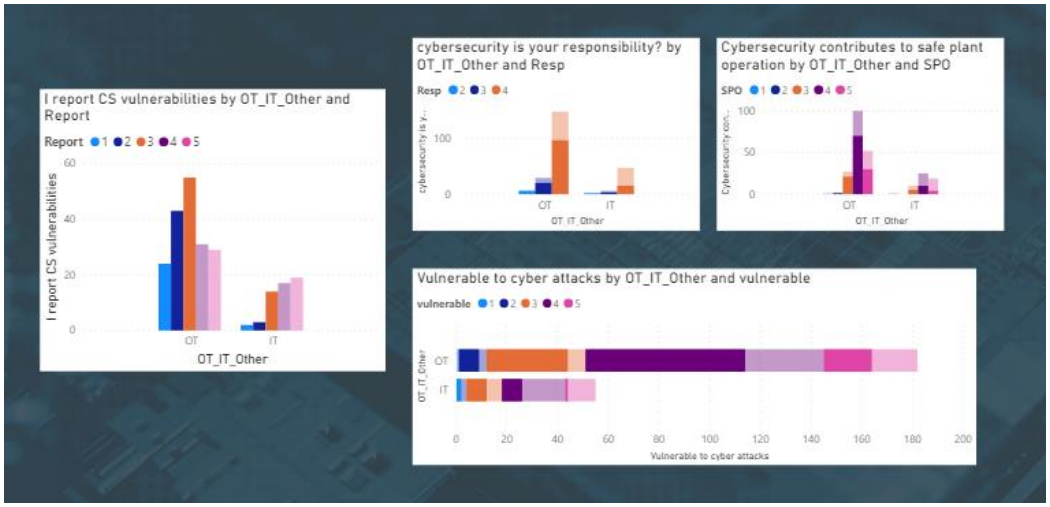


Figure 24: Reporting across positive indicators

Figure 25 supports figure 24 and shows that 15% of OT staff will do nothing if they identify a vulnerability and in IT 13% will do nothing. This was a multi-choice option and while not excessively high, it is still a cause for concern. Behavior in the OT environment while not being bad, is not particularly good (except for reading awareness messages) which shows there is room for improvement. It is going to be very important to understand what are the drivers of these behaviours using behaviour models to see who we can target interventions to address the root causes. Understanding the behaviours may require some interviews or a deep dive with some of the

groups that responded. In contrast figure 22 shows that 24% of staff would disable their antivirus in OT if they could.

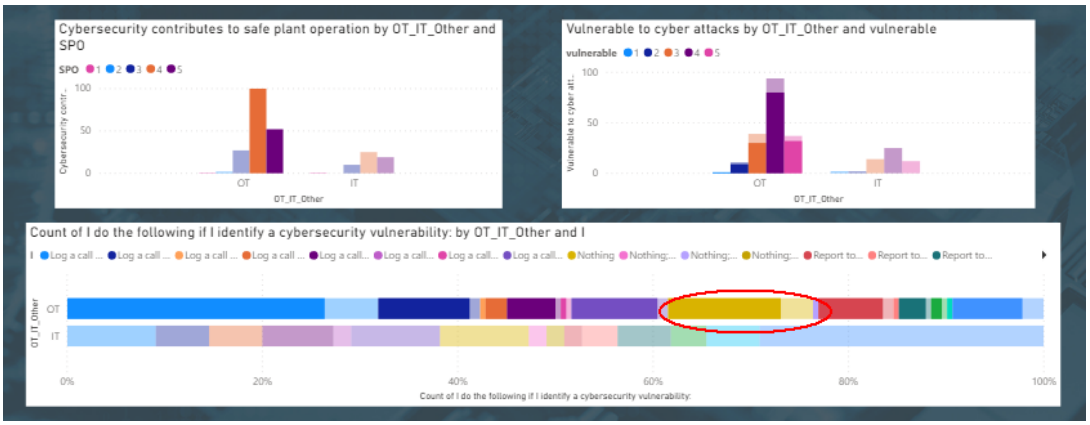


Figure 25: Individual response to cybersecurity vulnerability

While this number is not the majority, it is concerning. From the open comments section, there is concern that insider threat and sabotage are real and one of our biggest risks. The ENISA study (2017) highlighted the trade-off between performance and security objectives, and a few people stated they would turn of their antivirus/antimalware services as it impacted their objectives significantly [33]. There is also the perception that cybersecurity is someone else's problem, and is supported by the analysis around responsibility, reporting, and leadership, with OT and the rest of the business at large who consider it a Group IT problem.

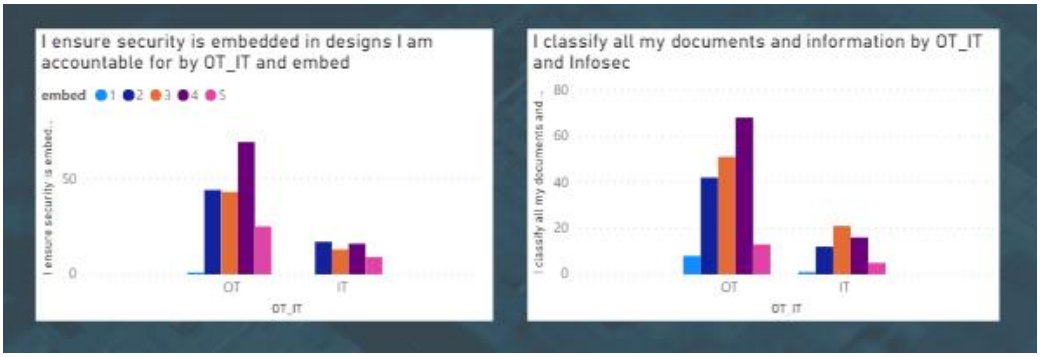


Figure 26: Embed security in design and classify documents

Figure 26 shows that 52% of respondents in the OT environment include security in the design of solutions and 45% classify their documentation. Group IT do not design many solutions but rather implement solutions and this could account for their poor response and they also have poor practice for classification of documents. OT staff that do not embed security in solutions are largely not involved in cybersecurity. This behaviour could be exacerbated by the processes in engineering not catering for cybersecurity and the low level of cybersecurity knowledge and maturity in the OT environment.

4.2.5 Organisation

The two most important observations under organizational analysis relate to accountability and budgeting. 66% of people do not know who is accountable for cybersecurity, which is complicated in a utility the size of Eskom as there are competing priorities in IT and OT safety vs availability, best effort vs low latency deterministic (Engineers *et al.*>, 2016) and general visibility of IT Security processes vs engineering OT cyber processes as shown in figure 27.

Figure 27: Observations related to organisation

It is also clear that budgeting for cybersecurity is generally not given high priority, again stable technologies, air-gapped systems, analogue redundancy all do not help this trend. Due to the information security awareness campaigns, the counterintuitive good results for the organisation embracing cybersecurity culture shows a healthy picture for cybersecurity culture in OT- postulation most definitely, but probably very close to the truth.

People believe that the organisation is behind technology yet in the process and technology results show a high dependence and confidence in technology that is not at the cutting edge. From the open comments, it is clear that there is an enterprise need for more awareness and training from basic to advanced and catering from generic to specific.

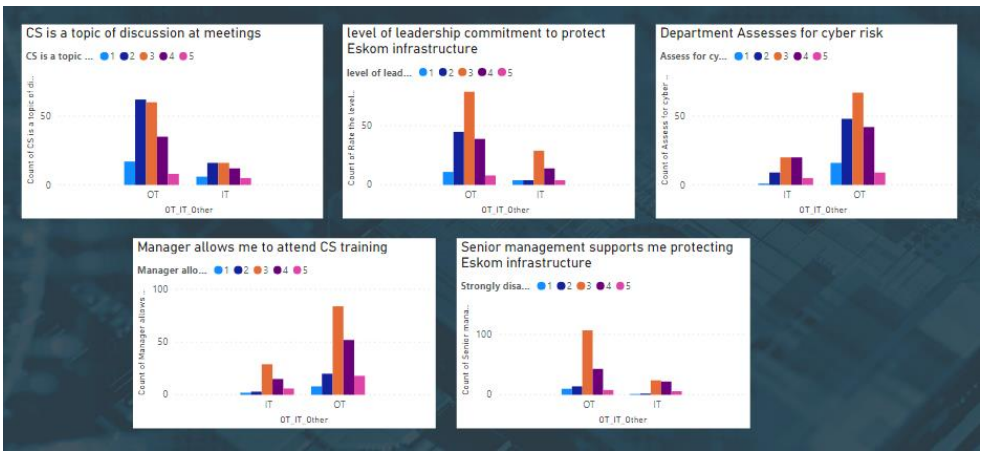


Figure 288: Leadership observations

Insider threat is considered one of the biggest threats to security in Eskom and the need for collaboration between IT and OT has been raised numerous times. In general, IT have results that are more favourable in all measures shown in figure 28. It is generally accepted that budgeting for cybersecurity speaks directly to organizational commitment and was highlighted in two independent external assessments conducted on the organisation.

Figure 299: Remote Access

The organisation does permit remote access to the industrial control network by external service providers and while there are standards in place, this is an important threat vector especially when one looks at open USB ports, management of sessions, potential backdoors into critical systems- the results are largely positive in that the majority (64%) is via managed connections and no remote connections allowed, however 34% is a large percentage for uncontrolled remote sessions. Remote access in IT has a similar risk profile to OT, which is alarming as the remote access policy was developed by GIT (figure 29). From the open comments section, some staff believe that IT and OT should be kept separate, while there is an increasing trend towards convergence worldwide. Some staff want frequent cybersecurity alert reports on attacks Eskom experienced, again there are different levels of cybersecurity knowledge and maturity in the business, but in general a more proactive approach to cybersecurity.

4.2.6 Leadership

The analysis of leadership highlighted some interesting insights, which when presented to senior management elicited a variety of responses like acceptance, surprise and defensiveness. This is a complex situation, as one needs to convince leadership to support something that they naturally feel they are good at, but the observations indicate there is a lot of room for improvement.

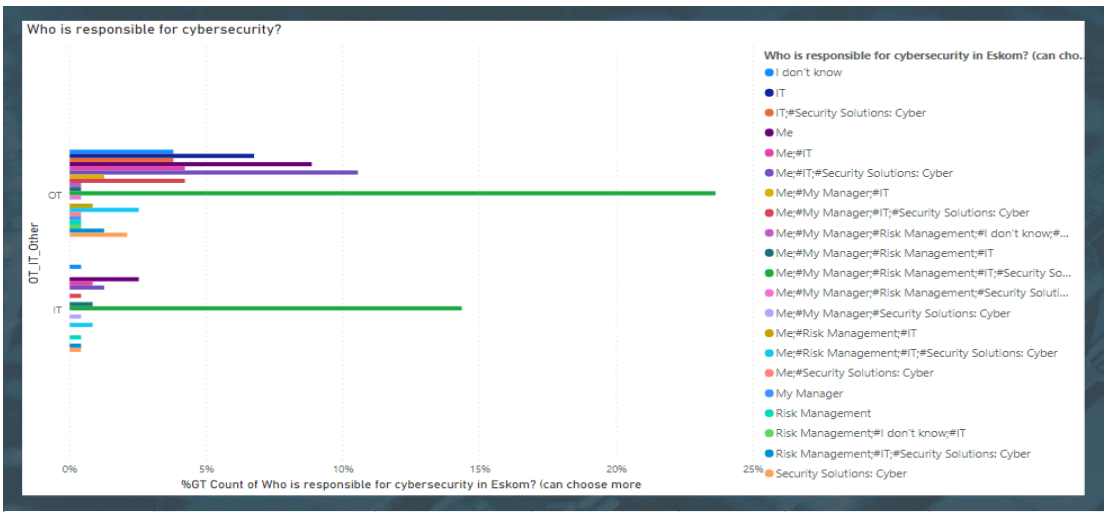


Figure 30: Responsibility for cybersecurity

Responsibility for cybersecurity in OT is very broadly spread while IT is more consistent as shown in figure 30. The most obvious answer was a combination of me, my manager, risk, IT, CS CoE. What is interesting to see is that there is quite a spread for both OT and other. In OT, the second most popular response was me, SSC CoE and IT followed by me and then IT. A far higher percentage of people in OT did not know who was responsible for cybersecurity in OT over IT. In IT, the second most popular choice was 'Me'. The spread from figure 30 correlates well to figure 27 under organisation, which shows that the organisation is also not clear on who is accountable for cybersecurity. Section 2.1 describes the confusion over security mandates and the need to have clear accountability in the organisation, which is supported in figure 30 and 24.

Figure 28 shows that the overall leadership perception of cybersecurity is low in OT, while IT leadership commitment shows a slightly more positive trend. Leadership in OT is more reactive with managers showing positive support for things like training and protecting infrastructure, things that do not require any real effort on their parts. A similar trend is seen in IT. For measures that require management to take the lead and drive, like facilitating cybersecurity discussions or assessing the department for cybersecurity risk, we see a more negative than positive trend in OT and a similar trend is also seen in IT quite surprisingly.

Figure 31: Management response to cyber-risk

Figure 31 shows the responses of management when approached with a cybersecurity concern with logging a call to IT being the most common response followed by using the risk management process. In IT, logging a fault and management proactively investigating the risk with you tied as the top responses showing clarity of process and maturity of leadership response. IT is responsible for IT security and tend to take a cyber-incident quite seriously as the accountability stops with them. In other words, leadership does not actively do anything, but if you raise a request or require support, they will help. In OT, there is a high dependence on OEMs for vulnerabilities and patch management and they are usually the first call. Figure 31 also relates to process and technology and how there is no standard way of logging a cybersecurity incident or vulnerability and a similar response is seen in figure 30 which shows responsibility for cybersecurity. Unclear responsibility and inconsistent reporting processes have a direct relationship to the poor reporting behaviour as seen in section 4.2.4. Eight percent of OT managers are not interested in cyber-risks or will tell their staff they are not IT people, this is a very poor reflection on them and shows they also have not internalized their own responsibility towards cybersecurity in their sections, while only 1% of responses in IT reflect this behavior. Figure 25 also shows how the behaviour of staff is also risky in that 15% of them do not report vulnerabilities. With individuals and management both showing risky behaviour and attitudes, a convergence of this behaviour may result in an incident.

4.2.7 Process and Technology

It is clear that the most mature processes for logging of cyber incidents remain the IT logging a call process and the Integrated Risk Management (IRM) process. This was clearly seen in the previous analysis in figures 30 and 31. There is a high dependence and confidence in technology. This could potentially be a driver for risky behaviour if individuals feel they are fully protected, they will take risks based on a false sense of security.

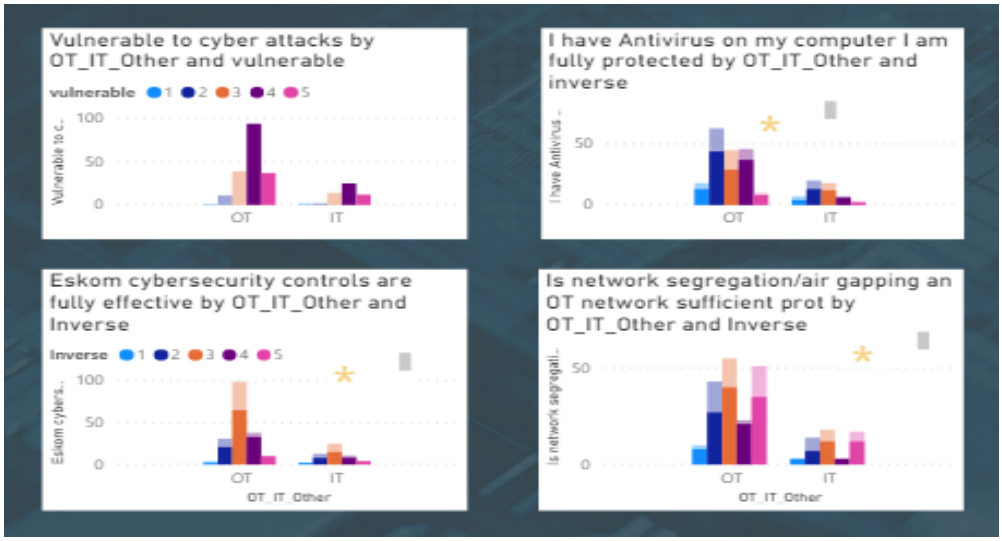


Figure 32: Process and Technology observations

The large number of respondents that believe that the Antivirus and cybersecurity controls implemented are fully effective evidences this in figure 32. It could be a testament to the automated controls and processes that are in place and the fact that Group IT and OT cybersecurity do not advertise attacks or breaches outside of their respective user groups. This creates the impression that there are no attacks. Only the high impact/consequence attacks are usually shared in a limited format with the larger organisation. Obfuscation is common in most security environments and is not unique to Eskom. Network segregation or air-gapping is a technique used in the operational environment to ensure that data does not traverse across networks and is usually implemented using a demilitarized zone (DMZ). It is largely considered by many in the plant environment to be very effective at keeping the network safe, as there is no direct connections to the corporate network or the internet.

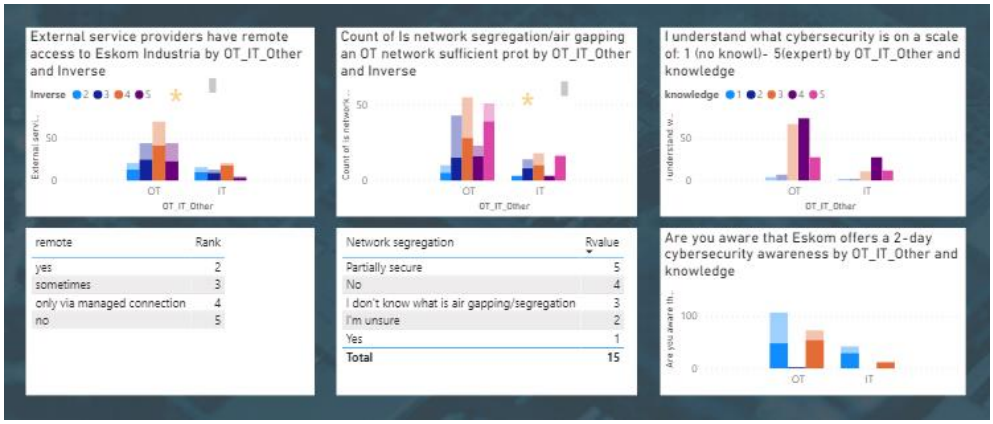


Figure 33: Remote connections and network segregation

It is widely accepted that network segregation is partially secure but when selecting people with good to excellent cybersecurity knowledge there is a significant amount (26%) who are aware of the

cybersecurity standard but who believe it is fully effective, are not sure what it is and are not sure as to its effectiveness seen in figure 33. Some of this sample are the people who are responsible for the configuration and safe operation of these systems. A similar trend is also seen in IT. The process for remote connections into Eskom is also quite erratic. On the Group IT, side there is a higher amount of unmanaged remote access connections which is probably due to the number of external service providers and SLA's we have externally. Figure 25 also highlights the multitude options of logging a cybersecurity incident, with many people choosing to do nothing due to lack of support from management, unclear reporting channels, unclear responsibility and accountability. Figure 27 also shows that 55% of staff believe that Eskom is lagging behind technology advancements, but they still believe that Eskom is fully protected.

From the open comments, some staff felt that Eskom's internet security policy, needed to be stricter with reference to social media access and general access. There was also suspicion from staff around third party access to their laptops and monitoring of their activities. This was also raised at strategic level about the balance between cybersecurity controls and monitoring versus data privacy. Some people did not believe that the current information security solutions were good and suggested alternatives. As mentioned earlier there was a vast spectrum of respondents some with advanced knowledge to basic and this showed in the open responses. Figure 26 under behaviours also relates to process and technology as embedding security into design needs to be a part of engineering design processes, however the organisation is not at that point yet as most of our plant is not fully digital. Information security classification processes while quite mature and integrated into documentation management processes, is also not as entrenched as we would have thought. Previous data loss prevention (DLP) solutions were not very successful with performance, ease of use, training all contributing to its uptake.

4.2.8 Summary of analysis

Due to Eskom being an organisation that manages critical infrastructure and consequently critical service delivery, the culture overall seems to align to this reality. The open comments section had good insights as people could express their views freely. One of the open comments was that the questionnaire did not clearly differentiate whether it was IT or OT network related. This was due to the CoE not being able to get a list of OT people. This is still a complex undertaking for an organisation of this size and unclear role clarity.

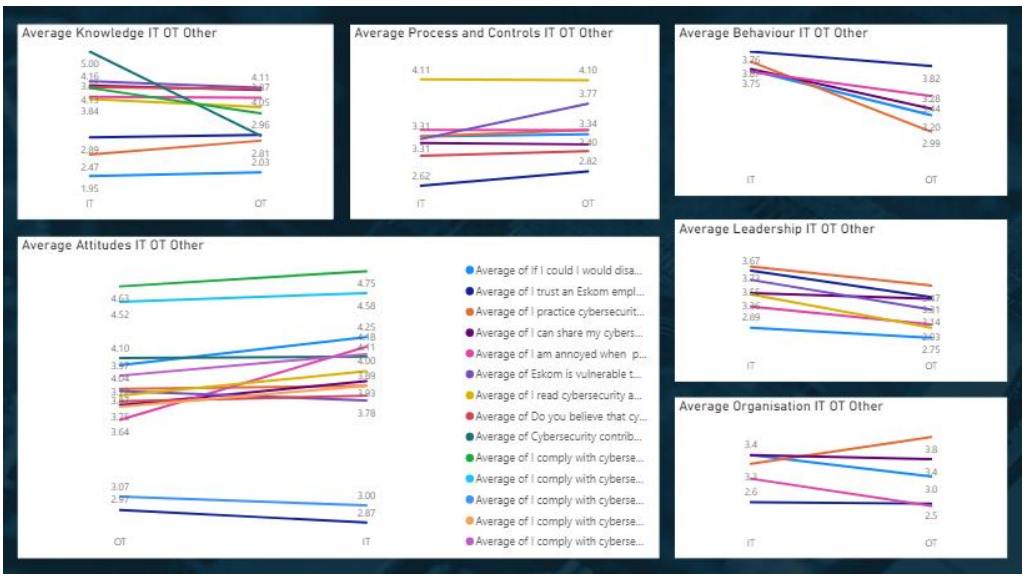


Figure 34: Average scores across all questions for IT and OT

There is an overwhelming need for awareness around cybersecurity and this came through clearly in the comments section and correlates well with the data collected under knowledge.
Figure 34 shows the average scores across all questions for IT and OT and is a powerful way to show where the most misalignment is and could help in prioritising high impact interventions for culture change. For knowledge, the biggest difference is in IT knowledge and computer skill, which is perfectly logical. The only aspect of knowledge that OT out-performed IT was related to the OT cybersecurity standard. The largest difference in behaviours was with regard to reporting with IT showing far better reporting behaviour. The gradient or steepness of the slope shows the greatest differences. There is least difference in reading awareness messages and sharing and IT showing greater accountability for cybersecurity in their personal capacity alluding to a higher level of maturity.

Attitudes are very similar for both IT and OT with annoyance for changing passwords showing the largest divergence. IT consistently outperformed OT on most measures, with OT showing marginally higher levels of trust than IT, better compliance, as they do not want Eskom to be impacted and with Eskom being vulnerable to cyber-attack. Overall process and technology seem fairly similar, with OT scoring slightly better on most, due to the high emphasis on safety and reliability. Remote access does seem to be better controlled in the OT environment than in IT. IT score marginally better at information classification, which makes sense, as it is an information security question. OT scored better on confidence in antivirus solutions. IT leadership is consistently at a higher level than OT with management allowing training being the least disparate. Both IT and OT believe that Eskom is behind technology with IT showing far better commitment to cybersecurity due to them having a budget for it. IT also are largely clear that they know who is responsible for cybersecurity, which speaks well to the lack of clarity regarding the operating model in OT.

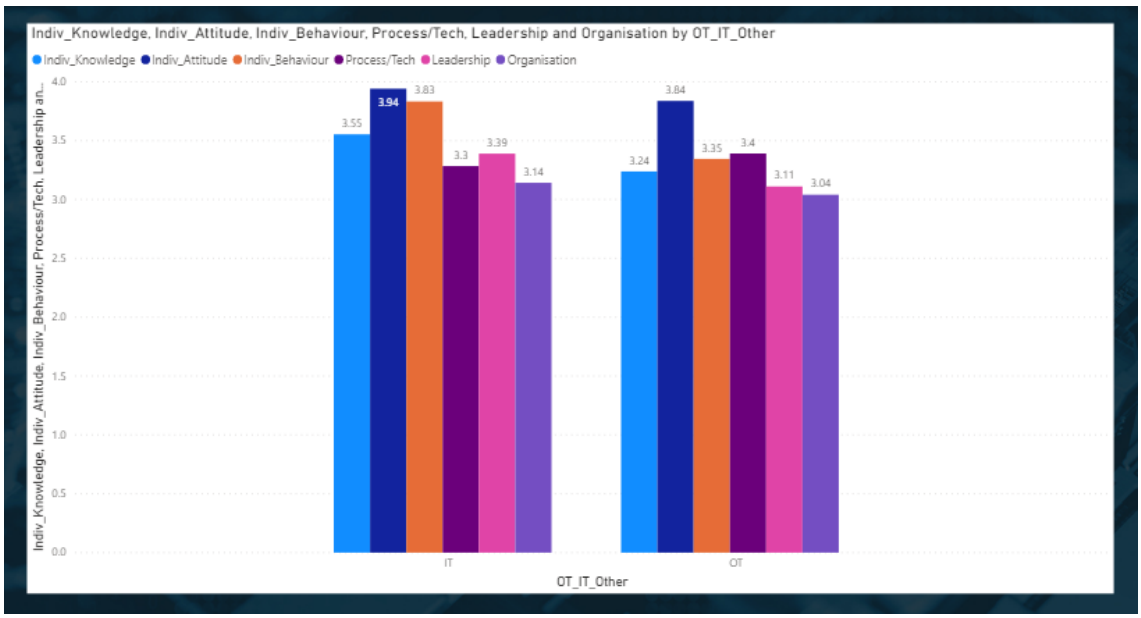


Figure 35: Rolled up summary scores across IT and OT

Figure 35 presents a rolled up view of all categories tested and show on the Likert scale how OT and IT score against each other. Taking an average of averages is not the most reliable of statistical measures but is a simplistic method of determining a score per category, hence the use of the previous line graphs with steep slopes showing the largest differences. Figure 34 and 35 can also be shown in a radar graph with three scores per criteria, OT, IT and target.

There are many scales that show maturity levels of cybersecurity in an organisation, and these can be adopted to plot these scores on those models to determine at what level of cybersecurity culture

maturity the organisation is at. Appendix 8.8 shows examples of a few cybersecurity maturity ratings and describe the different maturity levels at each rating point. It is easier to use a 5-dimension scale as it links directly to the scoring system of this study. Some of the scales investigated are summarised in the table below with graphics found in the appendix 8.8.

Source	Level 1	Level 2	Level 3	Level 4	Level 5
Security Architect Partners [99]	Initial	Developing	Defined	Managed	Optimised
Luiijf, E [100]	Unaware	Fragmented	Top Down	Pervasive	Networked
CMMI [76]	Initial	Repeatable	Defined	Managed	Optimising
Lizlance [101][3]	Vulnerable	Reactive	Compliant	Proactive	Resilient
SSE-CMM [76]	Performed informally	Planned and tracked	Well defined	Quantitatively controlled	Continuously improving
C2M2 [102]	Ineffective	Developing	Good	Highly Effective	World class
NIST Cybersecurity framework [62]	Partial	Risk informed	Repeatable	Adaptable	

Table 3: Maturity stages of culture (adapted)

On average Eskom is at a Level 3 from figure 35 but figure 34 shows the individual criteria across IT and OT moving between a Level 2 to Level 4. The results and observations are a fair assessment of the current culture of cybersecurity being one of compliance, with direction from the top but without the self- direction and pervasive sense of ownership seen at higher Levels. This study is in no form a maturity framework to be applied in other environments. What we have described here is an attempt to relate this study to an overall gap assessment. Culture is but one aspect of maturity frameworks, and a questionnaire is a part of assessing a maturity framework which can also include interviews, observations and metrics.

Our goal is to influence behaviours to move to a proactive form of adherence rather than compliance which is usually fear driven, and eventually to a networked leading and resilient organisation with strong group dynamics where staff look out for each other. When using cybersecurity maturity models, the target level needs to link to the risk profile of the organisation with a higher level needed as the risk increases, hence it is not necessary to adopt a level 5 as an example for every category or criteria, it is dependent on business objectives and the effect of uncertainty on them [64].

[3] Based on Reason 1997 and Parker 2006

5 Recommendations

From the analysis it is clear that while the current culture is around a level 3 on a maturity scale, there are some areas that need to be at a higher level and it is essential to determine what level of maturity we need to be at. At present, the organisation has taken a view to aspire to move up one level and needs to create a plan to get there.

Skills audit and repurposing

The first step in changing the culture in the OT environment is to conduct a skills audit and firstly determine who our OT staff are and of these who have aptitude and attitude to undertake cybersecurity functions. We will need to build in a check to see who also have advanced computer skills and note these. A similar exercise can be performed in IT to find which IT personnel have OT experience and/or skills. This can then help us establish a pool of talent that can be developed to meet the skills gap we have identified.

Operating Model and Strategy

In parallel with the skills audit, the operating model for cybersecurity needs to be finalised and ratified at the highest level. The operating model should address whether security should be merged or kept separate. There is an operational aspect as well as a corporate/strategic role and these need to be defined. Should separate cybersecurity centres of excellence for IT and OT be established at a corporate level? Eskom is in a phase of transition and is busy restructuring and separating off their business units who will be fully responsible for their own operations and balance sheets. Corporate functions will be expected to fulfil a functional leader model role. It is the author's view that the CoE's should be converged as there is not enough skills to populate two CoE's, so there is both a skills benefit as well as financial due to limiting duplication of effort and resources. Many of the respondents also supported the need for better collaboration between OT and IT. This is currently being addressed and proposals are being compared to other utilities and international best practice. Many other utilities are looking at improving overall security culture and this would require convergence of IT, OT and physical security. The nuclear sector supported by organisations like the IAEA have a number of documents and initiatives driving this.

CoEs perform a shaping, leading and specialised servicing function whereas divisions are required to perform a safeguarding and servicing function. Another key outcome from this exercise will be the development of a RACI matrix, which defines who is responsible, accountable, consulted and informed for the various processes. This will greatly influence and alleviate the issue of role clarity and accountability as identified in the questionnaire. This will also empower leadership to confidently act on their mandates, without fear of overstepping authority and territory. There will also be a need for a corporate cyber ops team to manage an integrated security operations centre (physical, IT, OT) the level of integration to be discussed and approved. A cybersecurity strategy should have a converged approach to dealing with cyber-risk and should be aligned with the organisations objectives and goals.

Training and Awareness

Traditionally training and awareness programs was seen as the main driver of culture transformation. It is still one of the most critical components but needs to be tailored for the different needs of the organisation at various levels. Currently information security and OT cybersecurity run these independently. It would be far more beneficial to have a collaborative solution and include elements of physical, information and operational technology security to create a model that comprehensively equips the larger organisation to identify, protect, detect and recover

from cyber-attack, irrespective of the threat vector. Observations from the questionnaire showed a divergent level of maturity and understanding of cybersecurity, but common to these subsets was the requirement for increased training and awareness. Awareness is usually a generic high-level activity that can be rolled out enterprise wide with high-level overview on security culture, but with more focused interventions then highlighting physical, IT and OT aspects. E-learning, gamification and simulations all form part of the suite of tools for expediting knowledge transfer. The figure below shows a possible view of the interventions that can be initiated. There is a need to improve communication, collaboration and the working relationship between security specialists and other functions in the organisation and increasing the awareness messages and channels for business to communicate and share concerns with security specialists either by access to the function, awareness messages and reporting [11].

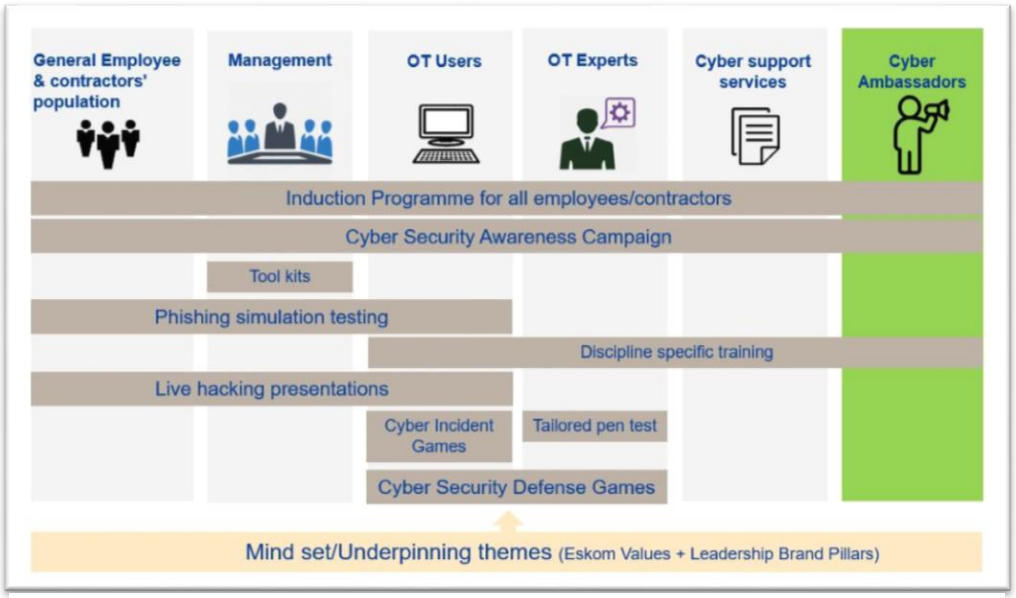


Figure 36: Training and awareness interventions (Eskom adapted) [25]

A very detailed fundamentals course has already been developed for the OT environment with the group also now converting this to digital for ease of use across any platform. Augmenting this with IT and physical domain knowledge will give us a good training information base. This can then be abstracted for different roles like middle management, risk practitioners, senior management. Very specific training for OT and IT staff can be procured at an enterprise level to capitalise on economies of scale. This can also give a CoE a view of very specialised skillsets that can be deployed as and when needed. Even if an OTS (off-the-shelf) culture transformation solution is procured, the work put in by the training team can be hosted on the solution as well. Buying a solution is attractive in that the built in metrics help track and influence what training and awareness is needed. Toolkits are also being developed to assist and empower managers to actively manage cybersecurity. By equipping leaders, they gain the respect of staff and their commitment. Identifying and equipping cyber- ambassadors is a great way to create and drive awareness at a tactical level.

Leadership

Leadership commitment to cybersecurity was considered to be low and according to Batteau there are three attributes that contribute to leadership perception: priority, participation and knowledge [6]. By developing leadership toolkits, we give leadership the tools they need to lead and direct cybersecurity. Toolkits bring the necessary knowledge in a meaningful easy way to leaders (demystify it, and reduce obfuscation which is prevalent in OT), which removes the stress of them

upskilling and finding material to discuss on cybersecurity. Once this impediment has been removed, leaders engage staff more effectively, and drive the cybersecurity agenda actively and this in turn creates the perception of priority being given to cybersecurity. Budgeting and resourcing is an important part of leadership commitment, and a CoE can have a role in helping OUs develop common structures and budget inputs around cybersecurity, which can assist in changing behaviours as commitment is then tangible and felt. By having common functions and structures across similar departments, it enables uniformity of approach to cybersecurity and over time this will increase maturity. At a strategic level, the operating model should identify the overall accountability for cybersecurity at CISO or CSO level. If we opt to have dual accountability for cybersecurity for OT and IT, we would need these leaders to be appointed at the same level with defined mandates. It is preferable to have a single chief officer accountable for cybersecurity across all areas as this immediately limits the 'blame game' when things go wrong, which is highly probable with increasing convergence.

Collaboration

Many studies referenced in Chapter 2 as well as verbal interviews conducted with security culture experts from the US confirm our observations that people view cybersecurity as someone else's problem [33]. This is also supported by the data on responsibility and accountability. CoE's have difficulty garnering support from business units due to the 'us' and 'them' mindset, operational pressures versus corporate requirements and lack of trust. It is extremely important to involve OT in solutions or processes that are proposed for rollout. In this way, a 'my' problem is transformed into an 'OUR' problem. This creates trust and buy-in from the business and may encourage business to reach out to corporate to assist them with their cybersecurity challenges by viewing them as solutions partners. This is already starting to happen in some areas of the business where insight and advice is requested and solutions and processes are collaboratively developed. Collaboration is critical in culture transformation, as group think plays a big role in how we behave as described in the theory of planned behaviour.

Governance, Reporting and Compliance

While some culture proponents do not feel that compliance and governance help culture, it is essential to have strong foundational elements to help create context and set the tone for cybersecurity. Governance structures send a message that cybersecurity is serious, and ensure that projects, designs, procurement of solutions and other cyber-related activities are robustly assessed before any form of additional investment. This ensures line of sight, application of economies of scale, justification of business cases and raising of cyber-risks at the correct levels. This all leads to a more positive view of organisational commitment. Unduly onerous governance processes may put a damper on issues; however not having governance means that cybersecurity will be managed in an adhoc manner.

We have poor reporting in Eskom influenced by unclear reporting processes, lack of feedback, lack of knowledge and unclear responsibility. Reporting should be acknowledged immediately and could have an incentive aspect. An example could be an automatic response thanking the user for their efforts. See figure 37 below for a simple button on the intranet on the homepage and associated incidents capture form with acknowledgement designed and presented by the author. Another easy way could be a hotline or link to the logging page from the desktop or a 'log a cyber issue' button on email client. It should be an easy process with multiple entry points for capture but a single convergence point for storing and dealing with the issues raised. The initial process should be very simple and is critical from a self-efficacy point of view as complicated processes are almost

guaranteed to fail. Reporting should be linked to a positive character trait and as seen from the analysis people are not driven by fear but are concerned with protection of assets, so the messaging should resonate with this sentiment. Existing processes like risk management and IT incident logging should be optimised to also collect cybersecurity reporting information.

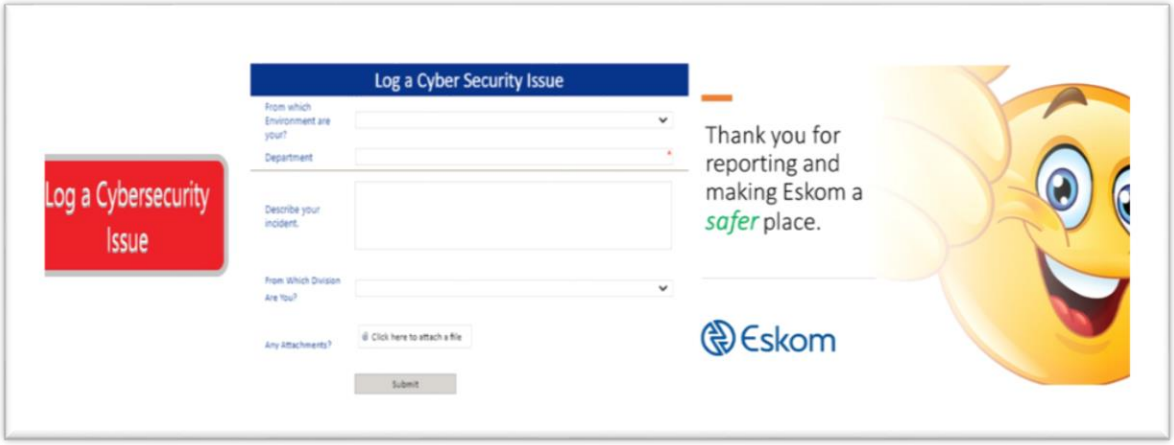


Figure 37: Web button for reporting

Compliance is traditionally associated with a fear culture while adherence has a more proactive positive spin, but still has a crucial role to play. According to the questionnaire, people comply because they care about Eskom and do not want compromise to the business assets, which leads to service disruption. This kind of pride can be leveraged to show how important adherence is to keeping Eskom safe. Traditionally compliance was measured by audits and assessments. There is an increasing drive to improve security culture in the nuclear sector by encouraging self-assessments. This is essentially an audit but done proactively by the business owners and shows great maturity and initiative. Audits have a poor reputation and are met with distrust and defensiveness, but this message needs to change, as it should be a tool for improvement, with a similar approach for self-assessments. The gaps identified help a department to focus on their shortcomings and continuously improve. The author recommends a cloud based compliance solution that caters for various standards that must be customisable to also capture internal requirements, legislation and standards like NIST, ISO 27000, IEC 62443 and so on. This solution should be configured to trigger an assessment that a department can undertake and upload evidence and self-score. The metrics should give valuable insight on where they need to improve and this has positive proactive culture and is measurable. For a large organisation, auditing every department can be very expensive and time consuming, but applying a sample based audit approach using the results from the self-assessment tool could be very efficient and cost effective. The audit department can then choose to focus on high scorers and their lessons learnt to help the rest of the business and low scorers to see how they can help them. Corporate offices can also assist to analyse and use tried solutions from better performing departments. The intention is purely for improvement.

Processes

Self- assessments can be integrated into the overall quality assurance programs of departments and this gives formality and commitment to improving culture. Performing any activity in an adhoc manner does not show belief and commitment to that activity adding long-term value to the organisation. It is important to formalise cybersecurity activities like self-assessments, cyber-asset management, governance structures and approval paths, vulnerability assessments, cyber-risk management and other processes related to protection, response, recovery and detection of cyber threats. It is more effective to embed these into existing mature business processes that employees

are already familiar with. An example of this could be cyber-risk management and the development of toolkits for the evaluation of cyber-risk. Certain business processes could have triggers that kick of a cybersecurity process, for example if an engineering department is implementing a digital solution, there should be a trigger to identify if the system is a critical cyber asset and if so then it should channel the relevant governance channel (like the security architecture authority) and secure by design process. Currently only staff who are involved in these committees follow these processes. It is important to engage the BPM (business process management) team to start to redesign the PCM's (process control modules) that should be integrating cybersecurity into their operations. Integration of cybersecurity into business processes will come with maturity, but a start would be to identify critical processes and start to engage and implement change on those. Technology solutions should be integrative and experts need to collaborate to ensure that functionality that is purchased integrate well with each other, are scalable and well supported for future proofing, at the same time developing strong relationships with service providers and OEM's who can accommodate specific security and technology requirements. An example of this could be upscaling a public key infrastructure project to not only include IIoT devices but also to partner with the suppliers of these devices to integrate with these projects. This culture of collaboration needs to be developed to ensure we limit working in silos on solutions but encourage working collaboratively at various levels.

General

These results are currently being presented at various forums in Eskom and at different levels in an effort to obtain executive support for interventions as part of a larger cybersecurity culture transformation journey. Based on the observations, the above points have been tabled as recommendations. This is the first step in a journey of culture transformation, which will no doubt be a multi-year project with continuous improvement being the mantra as the cyber threat will only be increasing as further adoption of digitilisation and convergence of technologies increase. While we have evaluated these dimensions in this round, and the metrics are extremely valuable, over time we will need to also develop further metrics for teamwork, cooperation and interdependency as maturity for cybersecurity grows. The figure below shows the journey map for cybersecurity transformation with the next step being the development of an integrated plan on how to achieve

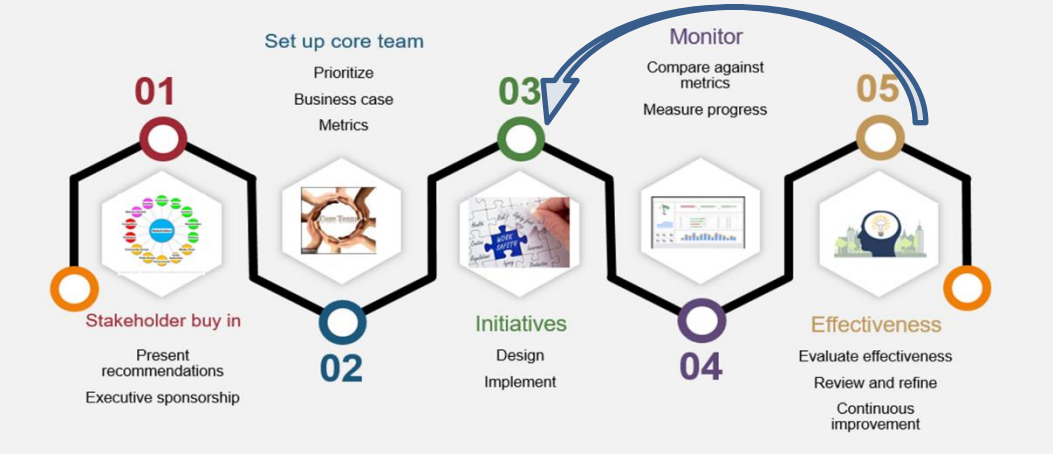


Figure 38: Culture transformation journey map

transformation. There are many lessons we can borrow from the nuclear industry and one of them is vigilance which is supported by improved knowledge and which will influence behaviour. Key partnerships will be established with departments responsible for learning, organizational design and culture, human performance, IT, OT, project management who will assist in prioritizing of

initiatives. Over time, focused initiatives will be implemented based on specific business needs and metrics established. These will be done in phases with effectiveness measured after each phased intervention with a feedback loop for improvements. Where needed deep dive sessions, interviews or observations will be conducted using COM-B, theory of planned behaviour or protection motivation theory to decode these.

6 Conclusion

The exercise of measuring cybersecurity culture has been an enjoyable learning curve, with some fresh insight gained into social sciences, psychology and research. The research objectives of this study were to:

a) Contextualise the cybersecurity mandate with emphasis on the role of IT, OT and physical security
b) Confirm whether user behaviour has an impact on the cyber-risk posture of an organisation (via literature)
c) Assess the cybersecurity culture of OT staff and comparing to IT, by investigating user perceptions, attitudes and behaviour by developing an instrument for measuring this.
d) Develop recommendations that will be incorporated into a program of work to catalyse cybersecurity transformation based on observations

The differences between IT and OT and the cybersecurity mandate was delineated by examining international standards and definitions and comparing these with Eskom documented information. It was determined that Eskom benchmarked their definitions internationally. The mandates were expanded based on the latest approved business cases and mandates at the time this research was conducted.

User behaviour and its impact on cybersecurity culture was confirmed by reviewing cybersecurity and information security culture research and the outcomes from these was implemented using a blended approach based on models for organisational design and culture most notably Schlienger and Schein [63]. Recent statistics as quoted in Chapter 1 also highlight the role of human behaviour in the threat landscape and rate it as a critical risk. Culture was broken down into knowledge, attitudes behaviours, beliefs as they relate to individuals, leadership, processes and technology and the overall organisation. This logical approach is well supported and yielded interesting results showing that there are variations in these dimensions across disciplines in Eskom (IT and OT) as well as the general staff.

A questionnaire was designed and implemented and the results analysed using data science methods mostly in the form of histograms and descriptive statistics. The qualitative data was transformed into numerical information that could be analysed and used to generate scores that in the future can be compared to view improvement. In general, Eskom cybersecurity culture is not bad at all, on average scoring at a three. Using maturity model descriptions it can loosely be translated as Defined, Top Down, Practicing, Compliant or Intermediate. In many of the dimensions measured, being at this level of maturity is adequate. However, there are many areas for improvement like reporting culture, leadership commitment and behaviour, dependence on technology, unclear processes and lack of clarity on accountability and training and awareness. Leadership, training, and awareness are probably the most referenced aspects of culture transformation and it was not surprising that it featured that highly in the observations. It is not essential to be excellent at all aspects of culture, but target scores should relate to organisational risk appetite and tolerance.

Recommendations were developed based on the observations ranging from the very simple high impact options to integrative complex solutions and will be prioritised by the development of a high-level plan, which will evolve into a program of work.

Criticism from funded research has said that many studies conducted by researchers with engineering background have analysed constructs in an effort to try to find something in employees that can be blamed for their non-compliant behaviours [11]. Humans are complex creatures and a variety of factors can influence a particular point of view, attitude or behaviour. We would hope to be able to unpack these drivers using interviews or deep dives with sample audience (or other effective techniques) and then designing interventions while measuring and testing effectiveness. It

is critical that we improve communication, collaboration, trust and work relations between OT and IT specialists, supporting staff and leadership, as there can be vulnerabilities in any of the sectors.

A combination of a human-centric approach, technology and processes will need to be adopted to be resilient in the age of 4IR (fourth industrial revolution). Employees and leadership need to be able to contextualize cyber-risk for their environments and understand how their behaviour and attitudes exacerbates or mitigates cyber-vulnerabilities. Training and awareness at multiple levels can assist to create understanding and provide resources with the tools to actively manage said risks. Lastly, we hope that from this work we will be able to formulate strategies, tools and initiatives that will provide the users with the capability, motivation and opportunities to react with the appropriate behaviour for any cyber-risky situation.

Future Work

It is recommended that future studies investigate a framework that caters for IT and OT security especially in organisations managing critical infrastructure. This could also link to the physical security culture as it pertains to cybersecurity adopted in the nuclear sector. Developing a cybersecurity culture capability model may also be worth investigating. Questions for the future should establish behaviours/attitudes/beliefs and the main drivers for them across the organisation at different levels, but also include **teamwork** and collaboration type questions, exercises and analysis to improve maturity across groups. It is challenging creating a one size fits all questionnaire, but at a strategic level this is essential, and by including physical, IT and OT questions, one can get an overall sense of security and using the outcomes from the skill audits start to develop more targeted initiatives and metrics dependent on the environment assessed. Due to the unclear mandate of cybersecurity in this organisation, this approach could not be adopted for the current study, but it would be more beneficial to have a holistic security assessment at an organizational level. Despite this obstruction, the objectives of the research project were successfully negotiated and useful insights gained into cybersecurity culture, while highlighting areas for improvement, which will be the driver for an organisational cybersecurity culture transformation program.

7 Bibliography

[1] Eric Ehlers, “2018 Cybersecurity Report Spotlights Emerging Threats to OT Environments.” [Online]. Available: https://blogs.cisco.com/manufacturing/2018-cybersecurity-report-spotlights-emerging-threats-to-ot-environments. [Accessed: 22-Jul-2018].

[2] “90% of cyberattacks traced back to human error: Making cybersecurity a workplace culture,” *Online*, 2017. [Online]. Available: https://www.newhorizons.com/article/90-of-cyberattacks-traced-back-to-human-error-making-cybersecurity-a-workplace-culture. [Accessed: 25-Jun-2018].

[3] “Critical Infrastructure Protection Act 8 of 2019 (English / isiXhosa) | South African Government.” [Online]. Available: https://www.gov.za/documents/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019-0000. [Accessed: 19-Apr-2020].

[4] “What the Explosive Growth in ICS-Infrastructure Targeting Means for Security Leaders.” [Online]. Available: https://securityintelligence.com/posts/what-the-explosive-growth-in-ics-infrastructure-targeting-means-for-security-leaders/. [Accessed: 18-Apr-2020].

[5] “Number of ICS Vulnerabilities Continued to Increase in 2020: Report | SecurityWeek.Com.” [Online]. Available: https://www.securityweek.com/number-ics-vulnerabilities-continued-increase-2020-report. [Accessed: 04-Feb-2021].

[6] A. W. Batteau, “Creating a Culture of Enterprise Cybersecurity,” *Int. J. Bus. Anthropol.*, vol. 2, no. 2, 2011.

[7] Trudy Knockless, “5 Types of Cyber Attacks and how they affect your business - McSweeney & Ricci Massachusetts Insurance,” *Property Casualty 360.com*. [Online]. Available: http://mcsweeneyricci.com/5-types-cyber-attacks-affect-business/. [Accessed: 22-Sep-2017].

[8] G. White, “The Community Cyber Security Maturity Model,” in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)*, 2007, pp. 99–99.

[9] ITU-T X.1205, “Cybersecurity Definition.” [Online]. Available: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. [Accessed: 23-Jul-2018].

[10] “ISO/IEC 27032:2012(en), Information technology — Security techniques — Guidelines for cybersecurity.” [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en. [Accessed: 01-Nov-2020].

[11] ENISA, “Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity About ENISA Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity,” 2018. [Online]. Available: https://www.google.com/search?q=enisa+publications&rlz=1C1GCEU_enZA850ZA850&oq=enisa+publications&aqs=chrome..69i57.13504j0j4&sourceid=chrome&ie=UTF-8.

[12] Martin Kuppinger, “It’s not about security vs. safety – it is about security and safety - KuppingerCole.” [Online]. Available: https://www.kuppingercole.com/blog/kuppinger/its-not-about-security-vs-safety-it-is-about-security-and-safety. [Accessed: 09-Sep-2019].

[13] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” *Natl. Inst. Stand. Technol.*, pp. 1–41, 2014.

[14] NICCS, “Glossary | National Initiative for Cybersecurity Careers and Studies.” [Online]. Available: https://niccs.us-cert.gov/glossary. [Accessed: 24-Jul-2018].

[15] “Cybercrimes Bill | PMG.” [Online]. Available: https://pmg.org.za/bill/684/. [Accessed: 07-Nov-2020].

[16] State Security Agency, “The National Cybersecurity Policy Framework (NCPF),” *Gov. Gaz.*, no. 39475, pp. 1–30, 2015.

[17] K. Reegård, C. Blackett, and V. Katta, “The Concept of Cybersecurity Culture,” in *29th European Safety and Reliability Conference (ESREL)*, 2019.

[18] G. Wyss, P. Sholander, J. Darby, and J. Phelan, “Identifying and Defeating Blended Cyber-Physical Security Threats,” *Proc. 25th Australas. Conf. Inf. Syst. ACIS 2014*, 2014.

[19] T. Rakau, “Security Division Business Plan Revision 2, Confidential,” 2017. [Online]. Available: http://intranet.eskom.co.za/Pages/default.aspx.

[20] P. Groenewald, “Definition of Operational Technology (OT) and OT/IT Collaboration Accountabilities.” Eskom SCOT Committee, Johanesburg, p. 8, 2012.

[21] R. Moodley, “OT operating model- Confidential,” 2015. [Online]. Available: http://intranet.eskom.co.za/Pages/default.aspx.

[22] R. Moodley, “Cyber CoE: Operating model and framework May 2020- Confidential,” 2020. [Online]. Available: http://intranet.eskom.co.za/Pages/default.aspx.

[23] T. Campbell, “Industrial Control Systems,” *Practical Information Security Management*, 2016. [Online]. Available: http://link.springer.com/10.1007/978-1-4842-1685-9_13.

[24] S. Panguluri, T. D. Nelson, and R. P. Wyman, “Creating a Cyber Security Culture for Your Water/Waste Water Utility,” in *Cyber-Physical Security*, Springer International Publishing, 2017, pp. 133–159.

[25] Eskom Academy of Learning, “Business driven Action Learning Cyber Security Presentation - Confidential,” 2020. [Online]. Available: http://intranet.eskom.co.za/Pages/default.aspx.

[26] “Cyber Kill Chain® | Lockheed Martin.” [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed: 21-May-2020].

[27] “What is Stuxnet, who created it and how does it work? | CSO Online.” [Online]. Available: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html. [Accessed: 22-May-2020].

[28] “Stuxnet - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Stuxnet. [Accessed: 22-May-2020].

[29] “December 2015 Ukraine power grid cyberattack - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack. [Accessed: 23-May-2020].

[30] T. Menze, “THE STATE OF INDUSTRIAL CYBERSECURITY 2019,” *Industry Week*, 2019. [Online]. Available: https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2019/.

[31] “Most Industrial Cyber Incidents Down To Human Error | Silicon UK Tech News.” [Online]. Available: https://www.silicon.co.uk/security/cyberwar/industrial-cyber-incidents-human-error-281319. [Accessed: 23-May-2020].

[32] J. Opacki, “Building a Security Culture- Why Security Awareness Does Not Work and What to Do Instead,” *ISACA*, vol. 5, pp. 1–6, 2017.

[33] ENISA, “Cyber Security Culture in organisations — ENISA,” 2017. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

[Accessed: 06-Aug-2019].

[34] K. Huang and K. Pearlson, “For What Technology Can’t Fix: Building a Model of Organizational Cybersecurity Culture,” in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[35] P. A. de F. Pereira, “Creating and Defining a Culture of Security- The human factor,” *ISACA J.*, vol. 6, pp. 1–5, 2017.

[36] N. Sohrabi Safa, R. Von Solms, and S. Furnell, “Information security policy compliance model in organizations,” *Comput. Secur.*, vol. 56, pp. 1–13, 2016.

[37] N. Gcaza, R. von Solms, M. M. Grobler, and J. J. van Vuuren, “A general morphological analysis: delineating a cyber-security culture,” *Inf. Comput. Secur.*, vol. 25, no. 3, pp. 259–278, 2017.

[38] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies,” *Comput. Secur.*, vol. 66, pp. 40–51, May 2017.

[39] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?,” 09-Jan-2019. [Online]. Available: http://arxiv.org/abs/1901.02672. [Accessed: 09-Mar-2020].

[40] J. W. Coffey *et al.*, “Ameliorating sources of human error in cybersecurity: Technological and human-centered approaches,” *29th Eur. Saf. Reliab. Conf.*, vol. 2017-March, no. December, pp. 1006–1015, 2017.

[41] European Union Agency for Network and Information Security, “NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies,” 2016.

[42] ISACA, *CISM Certification | Certified Information Security Manager | ISACA Review Manual*, 15th ed. Schaumburg: ISACA, 2015.

[43] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, “Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior,” *Int. J. Inf. Manage.*, vol. 45, pp. 13–24, Apr. 2019.

[44] “Theory of planned behavior - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Theory_of_planned_behavior. [Accessed: 03-May-2020].

[45] “Protection motivation theory - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Protection_motivation_theory. [Accessed: 02-May-2020].

[46] T. Halevi *et al.*, “Cultural and psychological factors in cyber-security,” in *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services - iiWAS ’16*, 2016, pp. 318–324.

[47] J. Van Niekerk and R. Von Solms, “A holistic framework for the fostering of an information security sub-culture in organizations,” *Issa*, pp. 1–13, 2005.

[48] L. Coles-Kemp, D. Ashenden, and K. O’Hara, “Why should I? Cybersecurity, the security of the state and the insecurity of the citizen,” *Polit. Gov.*, vol. 6, no. 2, pp. 41–48, Jun. 2018.

[49] I. Kirlappos, “Learning from " Shadow Security ": Understanding Non-Compliant Behaviours to Improve Information Security Management,” *Thesis PhD*, no. March, p. 286, 2016.

[50] NIST, “Risk management framework for information systems and organizations SP 800-37

Rev.2," 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[51] P. Trim and D. Upton, "Cyber Security Culture Counteracting Cyber Threats through Organizational Learning and Training," *Gower*, 2013.

[52] J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," *Proc. IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975.

[53] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 9, pp. 52–80, Jun. 2015.

[54] R. S. H. Piggin, "Governance, risk and compliance: impediments and opportunities for managing operational technology risk in industrial cyber security and safety," in *9th IET International Conference on System Safety and Cyber Security (2014)*, 2014, pp. 4.2.2-4.2.2.

[55] "Phishing Statistics 2020: 15 Phishing Stats to Help You Avoid Getting Reeled In | InfoSec Insights." [Online]. Available: https://sectigostore.com/blog/phishing-statistics-phishing-stats-to-help-avoid-getting-reeled-in/. [Accessed: 16-Jun-2021].

[56] K. T. T. Department, "Human Performance Tools- Confidential," 2011. [Online]. Available: http://intranet.eskom.co.za/Pages/default.aspx.

[57] C. Robinson, "Nuclear Safety Culture Traits," 2013. [Online]. Available: http://intranet.eskom.co.za/Pages/default.aspx.

[58] "SANS Institute: Information Security Resources." [Online]. Available: https://www.sans.org/information-security/. [Accessed: 22-Mar-2020].

[59] "Information security - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Information_security. [Accessed: 22-Mar-2020].

[60] A. Alhogail and A. Mirza, "Information security culture: A definition and a literature review," *2014 World Congr. Comput. Appl. Inf. Syst. WCCAIS 2014Alhogail, A., Mirza, A. (2014). Inf. Secur. Cult. A Defin. a Lit. Rev. 2014 World Congr. Comput. Appl. Inf. Syst. WC*, no. October, 2014.

[61] N. Gcaza and R. von Solms, "A strategy for a cybersecurity culture: A South African perspective," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 80, no. 1, pp. 1–17, 2017.

[62] S. Almuhammadi and M. Alsaleh, "Information Security Maturity Model for Nist Cyber Security Framework," *Comput. Sci. Inf. Technol.*, pp. 51–62, 2017.

[63] T. Schlienger and S. Teufel, "INFORMATION SECURITY CULTURE-FROM ANALYSIS TO CHANGE," *undefined*, 2003. [Online]. Available: https://www.researchgate.net/publication/220102979_Information_security_culture_From_analysis_to_change. [Accessed: 04-Apr-2020].

[64] J. S. Lim, A. Ahmad, S. Chang, and S. Maynard, "Embedding Information Security Culture Emerging Concerns and Challenges," 2010. [Online]. Available: https://www.researchgate.net/publication/221229226_Embedding_Information_Security_Culture_Emerging_Concerns_and_Challenges.

[65] A. Da Veiga, "A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument," *Proc. 2016 SAI Comput. Conf. SAI 2016*, pp. 1006–1015, 2016.

[66] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou, “Analysis of personal information security behavior and awareness,” *Comput. Secur.*, vol. 56, pp. 83–93, Feb. 2016.

[67] “Operational Technology - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Operational_Technology. [Accessed: 21-May-2018].

[68] “Industrial automation and control systems. | Download Scientific Diagram.” [Online]. Available: https://www.researchgate.net/figure/Industrial-automation-and-control-systems_fig1_333639056. [Accessed: 22-Mar-2020].

[69] “Welcome to Group Technology.” [Online]. Available: http://technology.eskom.co.za/assetm/Pages/Welcome-to-Group-Technology.aspx. [Accessed: 20-Jun-2018].

[70] R. Moodley, “Cyber security standard for Operational Technology,” 2016. [Online]. Available: http://intranet.eskom.co.za/Pages/default.aspx.

[71] R. Moodley, “OT Cyber Security Operational Plan 2016/2017-2017/2018- Confidential,” 2016. [Online]. Available: http://intranet.eskom.co.za/Pages/default.aspx.

[72] D. R. Kristian Steenstrup, Earl Perkins, Tim Zimmerman, Michael Patrick Moran and Efficiently, “Predicts 2017 : IT and OT Convergence Will Create New Challenges and Opportunities,” *Gartner*, 2017. [Online]. Available: https://www.gartner.com/en/documents/3531817/predicts-2017-it-and-ot-convergence-will-create-new-chal.

[73] W. Engineers, C. Teach, C. About, and I. T. Page, “Maverick * Research : What Engineers Can Teach CIOs About IT,” pp. 1–13, 2016.

[74] P. E. Proctor and R. Wagner, “Special Report: Cybersecurity at the Speed of Digital Business,” 2016. [Online]. Available: https://www.gartner.com/doc/3332117?srcId=1-6963644879&cm_sp=gi-_-cysec-_-srpage.

[75] H. Susanto, M. Almunawar, and Y. Tuan, “Information security management system standards: A comparative study of the big five,” *Int. J. Electr. Comput. Sci. IJECS-IJENS*, vol. 11, no. 5, pp. 23–29, 2011.

[76] Marc Levesque, “UNDERSTANDING CYBERSECURITY MATURITY MODELS WITHIN THE CONTEXT UNDERSTANDING CYBERSECURITY MATURITY MODELS WITHIN THE CONTEXT OF ENERGY,” *National Association of Regulatory Utility Commissioners (NARUC)*, 2020. [Online]. Available: https://pubs.naruc.org/pub.cfm?id=287AC0D5-155D-0A36-311A-67F7847F17F4.

[77] “HOME - CyberSecurity Hub.” [Online]. Available: https://www.cybersecurityhub.gov.za/. [Accessed: 14-Dec-2020].

[78] “What is GDPR? The summary guide to GDPR compliance in the UK | WIRED UK.” [Online]. Available: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018. [Accessed: 19-Apr-2020].

[79] European Parliament and Council, “General Data Protection Regulation (GDPR) – Official Legal Text.” [Online]. Available: https://gdpr-info.eu/. [Accessed: 09-Sep-2019].

[80] “What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019 | Digital Guardian.” [Online]. Available: https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection. [Accessed: 19-Apr-2020].

[81] “Protection of Personal Information Act Summary | POPIA.” [Online]. Available:

https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia. [Accessed: 09-Feb-2020].

[82] "The enforcement of POPI - Why is POPI compliance so important?" [Online]. Available: https://www.golegal.co.za/popi-compliance-enforcement/. [Accessed: 14-Dec-2020].

[83] "NCOP Passed the Cybercrimes Bill, Civil Union and the Science and Technology Laws Amendment Bills - Parliament of South Africa." [Online]. Available: https://www.parliament.gov.za/press-releases/ncop-passed-cybercrimes-bill-civil-union-and-science-and-technology-laws-amendment-bills. [Accessed: 14-Dec-2020].

[84] The Department of Justice and Constitutional Development, *Cybercrimes and Cybersecurity Bill*, no. 40487. 2017.

[85] "Critical Infrastructure Protection Act 8 of 2019 (English / isiXhosa) | South African Government." [Online]. Available: https://www.gov.za/documents/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019-0000. [Accessed: 07-Nov-2020].

[86] "Critical Infrastructure Act, 2019 - Government, Public Sector - South Africa." [Online]. Available: https://www.mondaq.com/southafrica/government-contracts-procurement-ppp/878390/critical-infrastructure-act-2019. [Accessed: 14-Dec-2020].

[87] T. S. Kelly, "Instilling a Culture of Security Starts With Information Governance feature," *ISACA J.*, vol. 5, pp. 1–5, 2018.

[88] A. O'Brien, J., Islam, S., Bao, S., Weng, F., Xiong, W., & Ma, "Literature review Literature review," *Lit. Rev.*, no. November, p. 7, 2013.

[89] "Culture and social cognition - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Culture_and_social_cognition. [Accessed: 22-Jun-2020].

[90] "What is a Likert Scale - Definition, example, characteristics, & advantages | QuestionPro." [Online]. Available: https://www.questionpro.com/blog/what-is-likert-scale/. [Accessed: 22-Jan-2021].

[91] "How to Design and Analyze a Survey - The Ultimate Guide to Forms and Surveys | Zapier." [Online]. Available: https://zapier.com/learn/forms-surveys/design-analyze-survey/. [Accessed: 26-Jan-2021].

[92] A. Joshi, S. Kale, S. Chandel, and D. Pal, "Likert Scale: Explored and Explained," *Br. J. Appl. Sci. Technol.*, vol. 7, no. 4, pp. 396–403, Jan. 2015.

[93] T. Young, "Questionnaires and Surveys," 2015. [Online]. Available: https://www.researchgate.net/publication/316228107_Questionnaires_and_Surveys.

[94] "Correlation Coefficient: Simple Definition, Formula, Easy Calculation Steps." [Online]. Available: https://www.statisticshowto.com/probability-and-statistics/correlation-coefficient-formula/. [Accessed: 26-Jan-2021].

[95] "Sample Size Calculator: Understanding Sample Sizes | SurveyMonkey." [Online]. Available: https://www.surveymonkey.com/mp/sample-size-calculator/. [Accessed: 27-Jan-2021].

[96] "Sample Size Calculator." [Online]. Available: https://www.calculator.net/sample-size-calculator.html. [Accessed: 27-Jan-2021].

[97] "Sample Size Calculator (Use in 60 Seconds) // Qualtrics." [Online]. Available: https://www.qualtrics.com/blog/calculating-sample-size/. [Accessed: 27-Jan-2021].

[98] “Five ways to calculate internal consistency.” [Online]. Available: https://drsimonj.svbtle.com/how-to-calculate-internal-consistency. [Accessed: 11-Feb-2021].

[99] D. Blum, “Security maturity assessments focus on people, process, and technology,” *Online*. [Online]. Available: https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/. [Accessed: 17-Dec-2020].

[100] E. Luiijf, “Five maturity levels of cyber security (source: WEF [7]). | Download Scientific Diagram.” [Online]. Available: https://www.researchgate.net/figure/Five-maturity-levels-of-cyber-security-source-WEF-7_fig2_274635658. [Accessed: 17-Dec-2020].

[101] E. Lance, “Cybersecurity Culture: A Definition and Maturity Model For Critical Infrastructure - Liz Lance.” [Online]. Available: https://www.lizlance.ca/cybersecurity-culture-a-definition-and-maturity-model-for-critical-infrastructure/. [Accessed: 17-Dec-2020].

[102] US Department of Energy, “CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2),” 2014. [Online]. Available: https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program.

8 Appendix

8.1 Ethics Approval

UNIVERSITY OF CAPE TOWN
IYUNIVESITHI YASEKAPA • UNIVERSITEIT VAN KAAPSTAD

Faculty of Science
University of Cape Town
Rondebosch
South Africa 7701

Tel: +27 21 650 2866/7
E-mail: Rachel.Wynberg@uct.ac.za

7 September 2018

Mr Abraham Parbhunath
Department of Computer Sciences

RE: ***An investigation into the maturity of cyber security culture in Operational Technology (OT) in Eskom***

Dear Mr Abraham Parbhunath

I am pleased to inform you that the Faculty of Science Research Ethics Committee has approved the above-named application for research ethics clearance, subject to the conditions listed below.

- Implement the measures described in your application to ensure that the process of your research is ethically sound; and
- Uphold ethical principles throughout all stages of the research, responding appropriately to unanticipated issues: please contact me if you need advice on ethical issues that arise.

Your approval code is: **FSREC 69 - 2018**

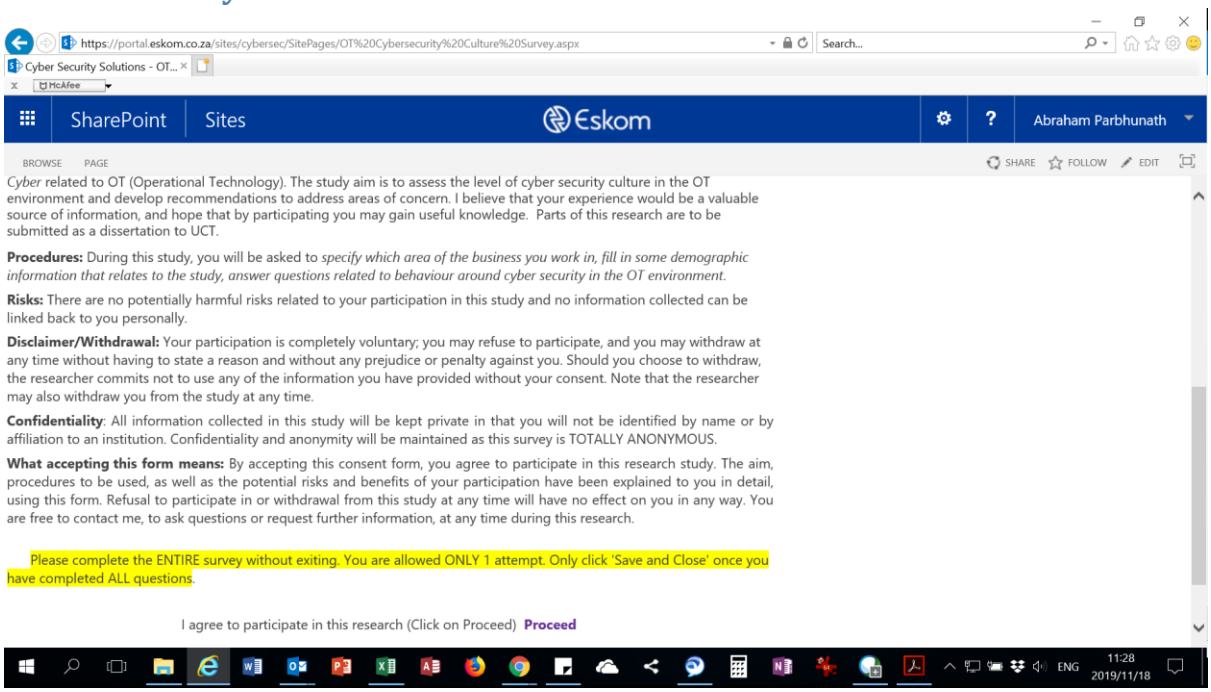
I wish you success in your research.

Yours sincerely

A/Prof Rachel Wynberg
Chair: Faculty of Science Research Ethics Committee

Cc: Prof Thomas Meyer (Supervisor)

8.2 Voluntary Consent



https://portal.eskom.co.za/sites/cybersec/SitePages/OT%20Cybersecurity%20Culture%20Survey.aspx

Cyber Security Solutions - OT...

SharePoint | Sites | Eskom | Abraham Parbhunath

BROWSE PAGE SHARE FOLLOW EDIT

Cyber related to OT (Operational Technology). The study aim is to assess the level of cyber security culture in the OT environment and develop recommendations to address areas of concern. I believe that your experience would be a valuable source of information, and hope that by participating you may gain useful knowledge. Parts of this research are to be submitted as a dissertation to UCT.

Procedures: During this study, you will be asked to *specify which area of the business you work in, fill in some demographic information that relates to the study, answer questions related to behaviour around cyber security in the OT environment.*

Risks: There are no potentially harmful risks related to your participation in this study and no information collected can be linked back to you personally.

Disclaimer/Withdrawal: Your participation is completely voluntary; you may refuse to participate, and you may withdraw at any time without having to state a reason and without any prejudice or penalty against you. Should you choose to withdraw, the researcher commits not to use any of the information you have provided without your consent. Note that the researcher may also withdraw you from the study at any time.

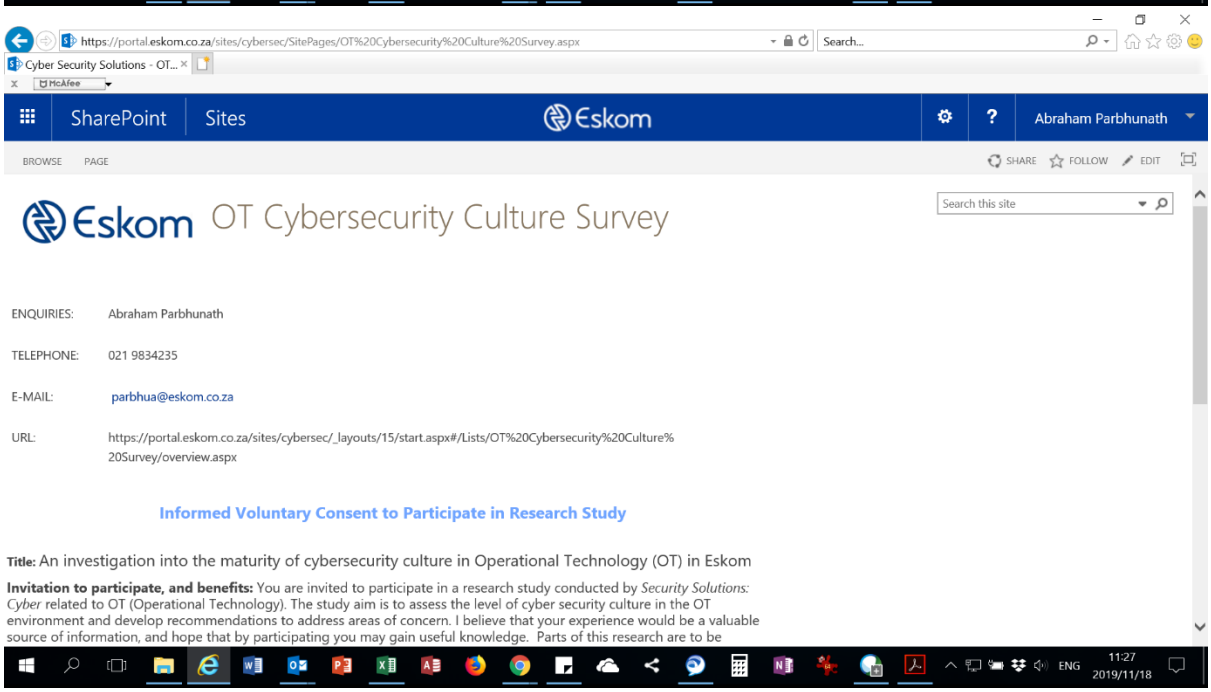
Confidentiality: All information collected in this study will be kept private in that you will not be identified by name or by affiliation to an institution. Confidentiality and anonymity will be maintained as this survey is TOTALLY ANONYMOUS.

What accepting this form means: By accepting this consent form, you agree to participate in this research study. The aim, procedures to be used, as well as the potential risks and benefits of your participation have been explained to you in detail, using this form. Refusal to participate in or withdrawal from this study at any time will have no effect on you in any way. You are free to contact me, to ask questions or request further information, at any time during this research.

Please complete the ENTIRE survey without exiting. You are allowed ONLY 1 attempt. Only click 'Save and Close' once you have completed ALL questions.

I agree to participate in this research (Click on Proceed) **Proceed**

ENG 11:28 2019/11/18



https://portal.eskom.co.za/sites/cybersec/SitePages/OT%20Cybersecurity%20Culture%20Survey.aspx

Cyber Security Solutions - OT...

SharePoint | Sites | Eskom | Abraham Parbhunath

BROWSE PAGE SHARE FOLLOW EDIT

Eskom OT Cybersecurity Culture Survey

Search this site

ENQUIRIES: Abraham Parbhunath

TELEPHONE: 021 9834235

E-MAIL: parbhua@eskom.co.za

URL: https://portal.eskom.co.za/sites/cybersec/_layouts/15/start.aspx#/Lists/OT%20Cybersecurity%20Culture%20Survey/overview.aspx

Informed Voluntary Consent to Participate in Research Study

Title: An investigation into the maturity of cybersecurity culture in Operational Technology (OT) in Eskom

Invitation to participate, and benefits: You are invited to participate in a research study conducted by *Security Solutions: Cyber* related to OT (Operational Technology). The study aim is to assess the level of cyber security culture in the OT environment and develop recommendations to address areas of concern. I believe that your experience would be a valuable source of information, and hope that by participating you may gain useful knowledge. Parts of this research are to be

ENG 11:27 2019/11/18

8.3 Questionnaire as implemented

	Question	Objective	Category	Scale / Choice
1	Division	Select Division type	Demographics	(Gx, Dx, Tx, Telecoms, Other)
	Select Gx Type			Coal NB, Fossil, Nuclear, Peaking
	Select Dx OU			GOU,WCOU,NCOU, FSOU KZNOU, LOU,ECOU, MOU, NWOU, HO
2	Group	To capture departments that did not fall in the above	Demographics	Capital, IT, Primary Energy, Risk and sustainability, Security, Technology, Other
3	Department Type	First differentiator between IT and OT	Demographics	IT, OT, Engineering, Other
4	Age		Demographics	18-25 25-35 35-45 45-55 55-65 Other
5	Gender		Demographics	M F Other
6	Task grading		Demographics	T/P 4-13 MPSG 14-18 E-Band and Above Contractor
7	I understand what cybersecurity is on a scale of: 1 (no knowledge) to 5 (expert)	What is employee perception of their knowledge?	Knowledge	1-5

8	I am involved in cybersecurity projects	Are they working on cybersecurity projects and a control on IT and OT experience	Knowledge	Y N
9	I practice cybersecurity in my day to day activities at work	There should be a correlation between 7 and 8. Can determine whether they mean information security.	Knowledge/self-efficacy	Strongly disagree to Strongly agree
10	I am interested to learn more about cybersecurity	Attitude and willingness to learn	Attitude	Strongly disagree to Strongly agree
11	Are you aware of the Operational Technology cybersecurity standard for OT?	Effectiveness of current awareness of the OT cybersecurity standard.	Knowledge	Y N
12	Are you aware that Eskom offers a 2-day cybersecurity awareness training that you can book via Zenzele?	Look at correlation between 11 and 12. Hopefully they have done the Eskom training. May need a control on 12 just to verify if they have done external may be more mature on Bradley curve	Knowledge	Y N
13	Do you have IT background/skills?	Determine if they have IT expertise	Knowledge	Y N
14	Do you have any Operational Technology (OT) background/skills?	Determine if they have OT expertise	Knowledge	Y N
15	What level of computer skill do you possess? 1 (basic) to 5 (expert)	Perception of computer literacy/expertise. Higher the literacy the higher the awareness.	Knowledge	1-5
16	I read cybersecurity awareness messages/ articles/ media	Do they actively acquire knowledge about cybersecurity	Behaviour	Strongly disagree to Strongly agree
17	I share this insight (from previous question)	Shows maturity from self-learning to sharing information links to group as well	Behaviour/ collaboration	Strongly disagree to Strongly agree

18	I scan USB/removable drives before using them	How risk averse is the user. Has impacts in OT. Can link to insider threat	Behaviour	Strongly disagree to Strongly agree
19	Do you have any antivirus/anti-malware software on your phone?	This is good practice and shows deliberation and acknowledgment of risk	Behaviour	Y N
20	I recognise SCAM/ phishing emails	Perception of their knowledge	Knowledge	Strongly disagree to Strongly agree
21	I am annoyed when prompted to insert a stronger password	relates to emotional state	Attitude	Strongly disagree to Strongly agree
22	I report cybersecurity vulnerabilities: 1 (never) to 5 (All of the time)	Maturity of user to cybersecurity risk	Behaviour/Vigilance	1-5
23	Eskom has good training and awareness on cybersecurity	Perception of organisational culture towards awareness and training	Attitude / beliefs	Strongly disagree to Strongly agree
24	If I could I would disable my antivirus because it slows down my pc.	Individual behaviour and risk appetite. Risk related to performance.	Attitude / values	Strongly disagree to Strongly agree
25	Eskom is vulnerable to cyber attacks	Perception of risk to business. Should inform behaviour. Should see correlation to 19-24	Attitude / perceptions	Strongly disagree to Strongly agree
26	What kind of cyber-attack is Eskom vulnerable to?	Tests their knowledge vs how their perceived knowledge level. There is a most correct answer	Knowledge	1. I don't know 2. Denial of service 3. Spoofing 4. Phishing 5. Ransomware 6. Options 2-5
27	I can share my cybersecurity concerns to the people I interact with	Relates to teamwork and interdependency	Attitude / values / norms / cognition	Strongly disagree to Strongly agree

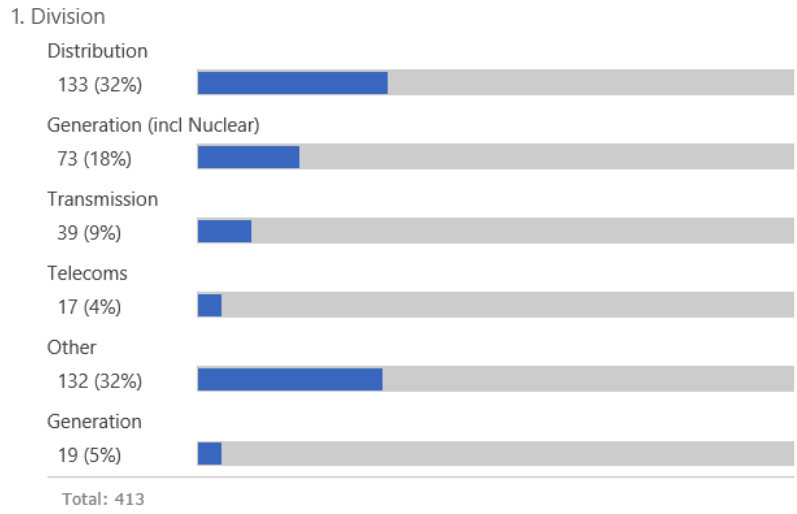
28	I trust an Eskom employee from corporate to perform assessments on my plant control systems	To check if Eskom site personnel trust Eskom employees at head office. If they do not, rolling out a functional leader model for cybersecurity management may be challenging	Attitude/ values / norms	Strongly disagree to Strongly agree
29	Cybersecurity is a topic of discussion in management meetings	Leadership focus on cybersecurity	Leadership /cognition	Strongly disagree to Strongly agree
30	Who is responsible for cybersecurity in Eskom? (can choose more than one)	Looking at sense of ownership for cybersecurity, looking to see if it is clear who is responsible- need to analyse spread	Leadership	Me, My Manager' Risk Management, I don't know, IT, Security Solutions: Cyber
31	My manager allows me to attend cybersecurity training	Leadership support for training. (Reactive)	Leadership	Strongly disagree to Strongly agree
32	Rate the level of leadership commitment to protect Eskom against Cyber attack	What is perception of leadership commitment to cybersecurity	Leadership	Very Low Low Medium High Very High
33	My department assesses for cyber-risk	Test for proactive leadership	Leadership	Strongly disagree to Strongly agree
34	If you approached your manager with a potential cyber-risk would he/she: (can select more than one option)	Clarity of processes and attitude of leadership to cybersecurity issues. We need to analyse spread to see if there is convergence.	Leadership	Proactively investigate the risk with you, Tell you to follow the risk process, Not be interested, Tell you he is not an IT person, Ask you to log a call,

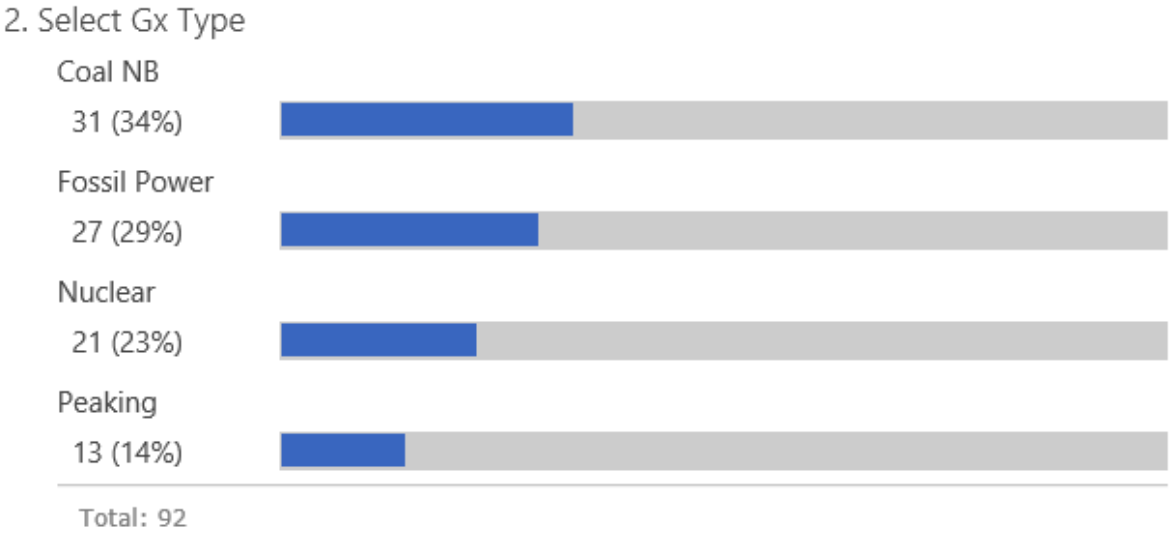
35	Senior management supports me in protecting Eskom's infrastructure by investigating cyber-risks that I report	Perception of senior leadership support for cybersecurity	Leadership	Strongly disagree to Strongly agree
36	I do the following if I identify a cybersecurity vulnerability: (multiple selections allowed)	Consistent processes and need to analyse spread. This is also a behaviour. We also wanted to see if the business recognises SSC CoE as a cybersecurity owner	Process/ Technology/ Behaviour	Nothing Log a call with IT Report to my supervisor Report to Risk practitioner Report to Security Solutions (Cyber)
37	Eskom cybersecurity controls are fully effective	Link this to personal behaviour. If they believe controls are effective they may take risks 18-22	Process/ Technology	Strongly disagree to Strongly agree
38	I have Antivirus on my computer. I am fully protected.	Same as 37. Also link to 25 where we see if they think Eskom is vulnerable	Process/ Technology	Strongly disagree to Strongly agree
39	Is network segregation/air gapping an OT network sufficient protection of an Industrial Control System (ICS)?	This should be linked to IT OT experience and knowledge. Filter out all results with no knowledge	Process/ Technology	No, I don't know what is air gapping / segregation, I'm unsure, Yes, Partially secure
40	I ensure security is embedded in designs I am accountable for	This should be linked to IT OT experience and knowledge. Filter out all results with no knowledge	Process/ Technology	Strongly disagree to Strongly agree I am not involved in design work
41	I classify all my documents and information (Controlled disclosure, confidential, etc.)	This relates to information security	Process/ Technology	Strongly disagree to Strongly agree
42	Cybersecurity contributes to safe plant operation	Testing if Eskom guardians at OT sites understand the link between safe plant operation and plant cybersecurity. If most understand the link… awareness may be	Process/ Technology	Strongly disagree to Strongly agree

		created using Eskom's safety principles		
43	It is clear to me who has overall accountability for Cybersecurity in Eskom	Is accountability for cybersecurity clear in Eskom?	Organisation	Strongly disagree to Strongly agree
44	My department budgets for cybersecurity	From previous findings. Financial planning correlates to commitment	Organisation	Strongly disagree to Strongly agree
45	Eskom organisational culture embraces cybersecurity risk	Perception of our larger organisational culture. There may be blurring with information security initiatives	Organisation	Strongly disagree to Strongly agree
46	ESKOM is ahead of Technology advancement and digitilisation	Perception of technology adoption. Can link to perception of technology controls	Organisation	Strongly disagree to Strongly agree
47	External service providers have remote access to Eskom Industrial control network	Remote access is a major challenge in OT. Are controls applied consistently?	Organisation / Process / Technology	Yes, Sometimes, only via managed connection, no
48	Please feel free to share your thoughts/ Suggestions/ Observations around cybersecurity culture	Open comments section at the behest of independent experts.		
49	Do you believe that cybersecurity is your responsibility?	Do respondents believe they have a responsibility to cybersecurity? Will link this to behaviour	Attitude/ Beliefs	Strongly disagree to Strongly agree
50	I comply with cybersecurity policies because:_(multi-selection question)	This question explores the driver of compliance to cybersecurity policy.	Individual	I don't care, I don’t want to be embarrassed, I don’t want Eskom to be impacted,

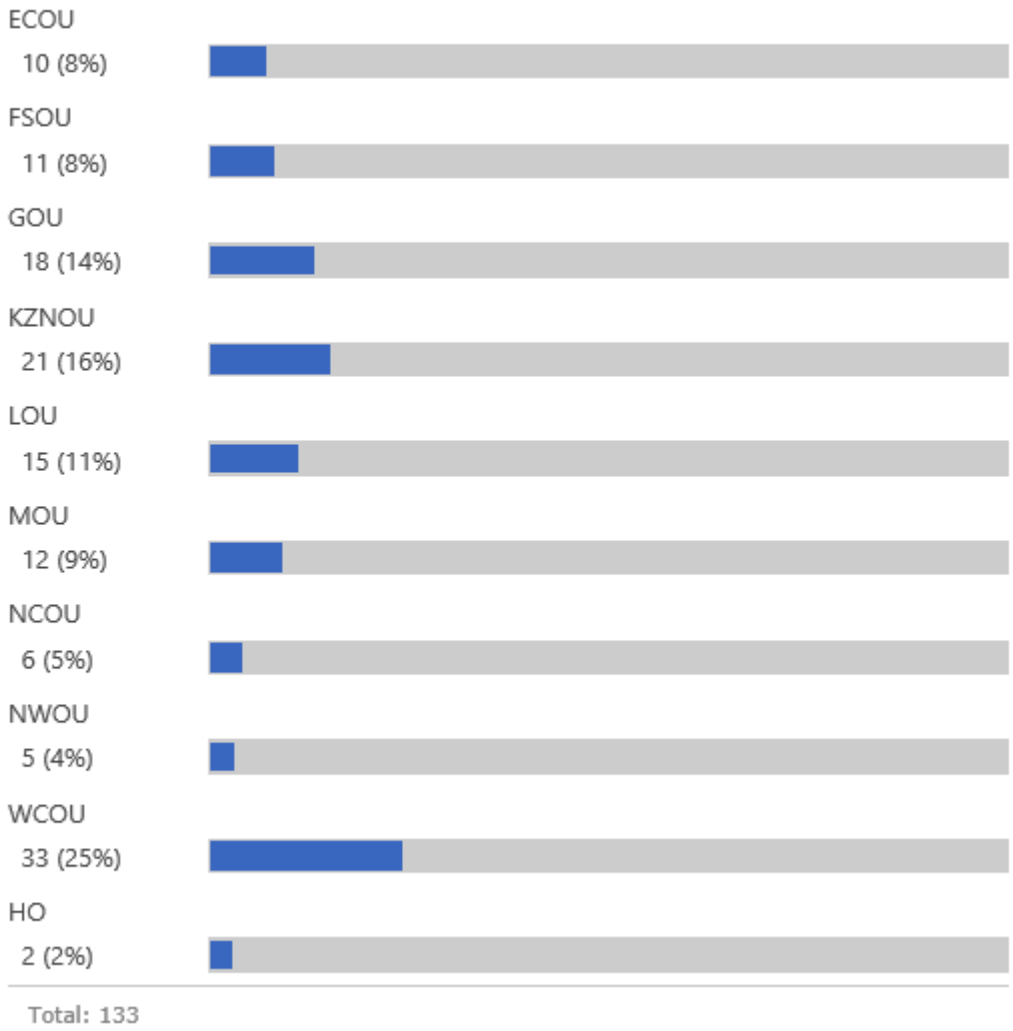
				I value my job, I fear the Consequences

8.4 Questionnaire Results

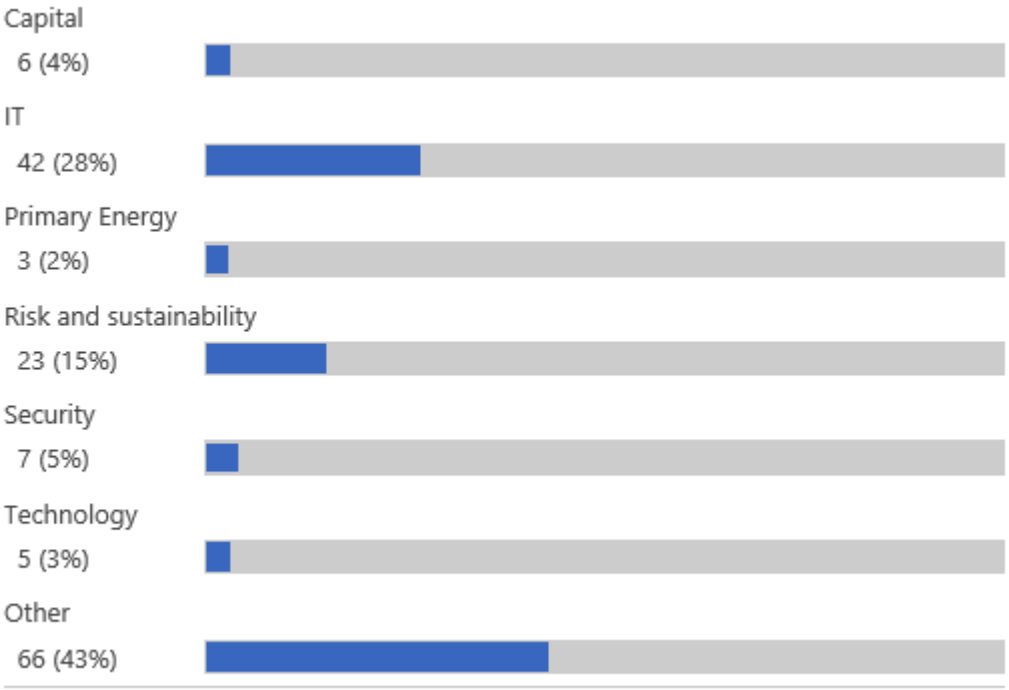




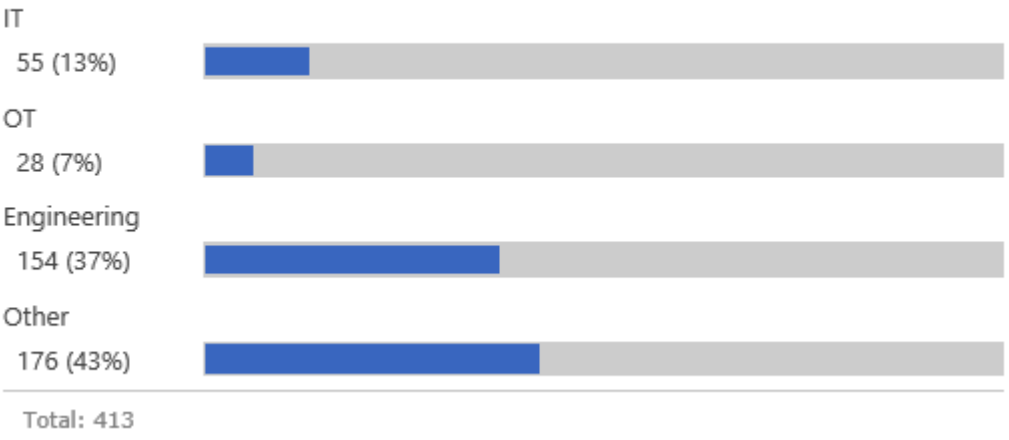
3. Select Dx OU



4. Group



5. Department Type



7. Gender

M

271 (66%)

F

140 (34%)

Other

2 (0%)

Total: 413

6. Age

18-25

0 (0%)

25-35

65 (16%)

35-45

107 (26%)

45-55

144 (35%)

55-65

97 (23%)

>65

0 (0%)

Total: 413

8. Task grading

T/P 4-13

227 (55%)

MPSG 14-18

176 (43%)

E-Band and Above

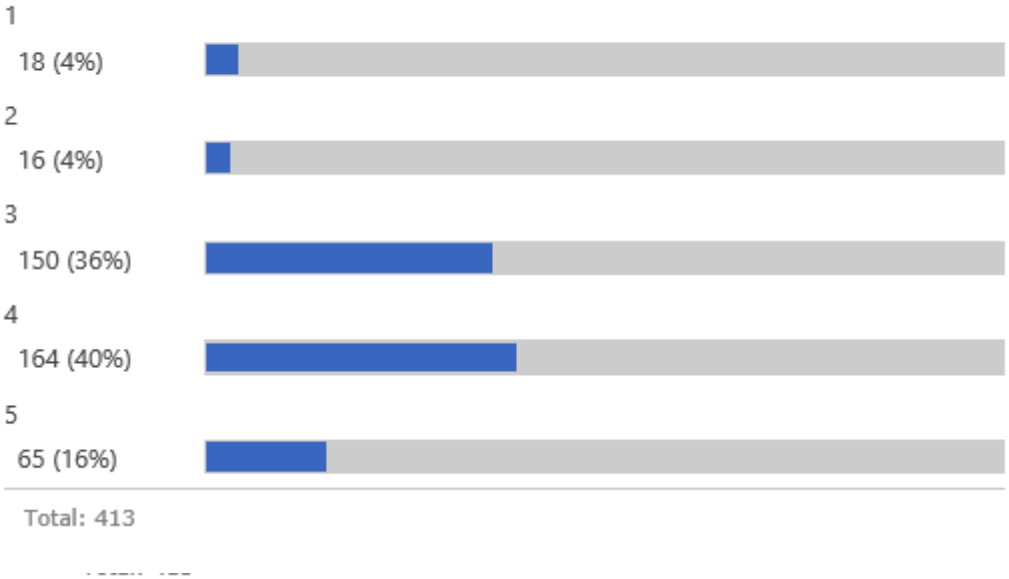
9 (2%)

Contractor

1 (0%)

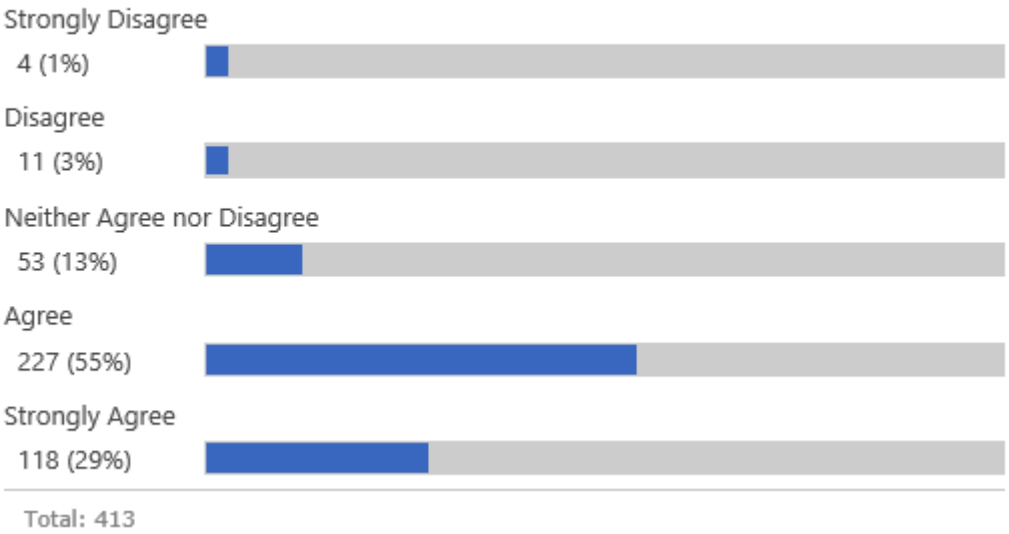
Total: 413

9. I understand what cybersecurity is on a scale of: 1 (no knowledge) to 5 (expert)

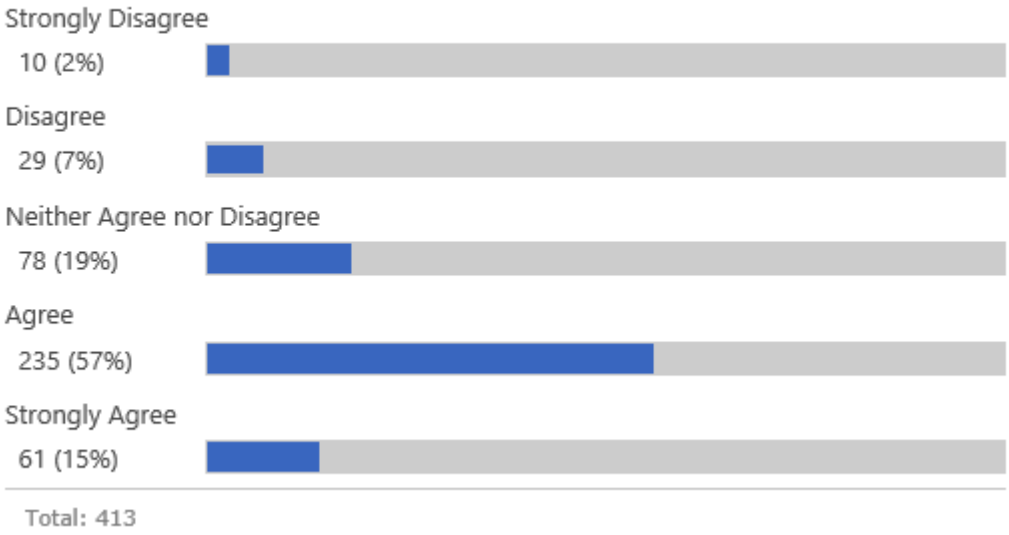


10. I am involved in cybersecurity projects

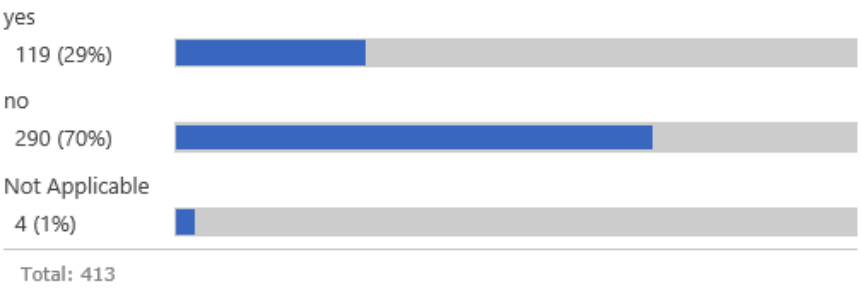
11. I am interested to learn more about cybersecurity



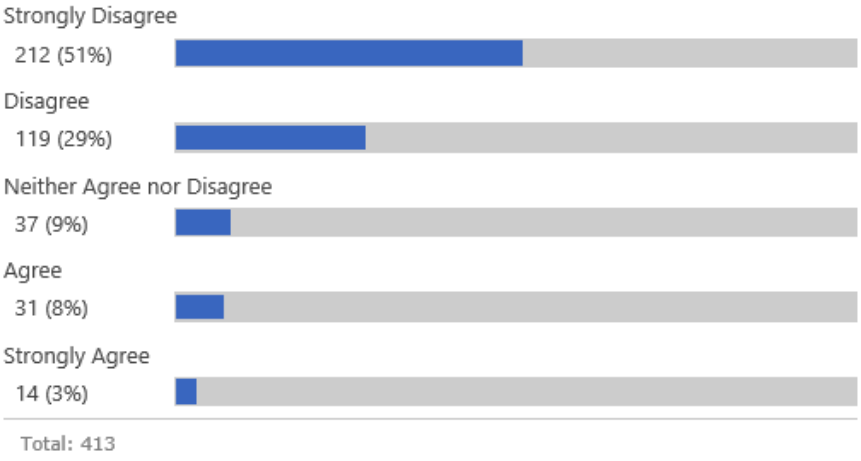
12. I can share my cybersecurity concerns to the people I interact with



13. Are you aware that Eskom offers a 2-day cybersecurity awareness training that you can book via Zenzele?



14. If I could I would disable my antivirus because it slows down my pc.



15. Do you have IT background/skills?

yes

183 (44%)

no

230 (56%)

Total: 413

16. I practice cybersecurity in my day to day activities at work

Strongly Disagree

13 (3%)

Disagree

33 (8%)

Neither Agree nor Disagree

79 (19%)

Agree

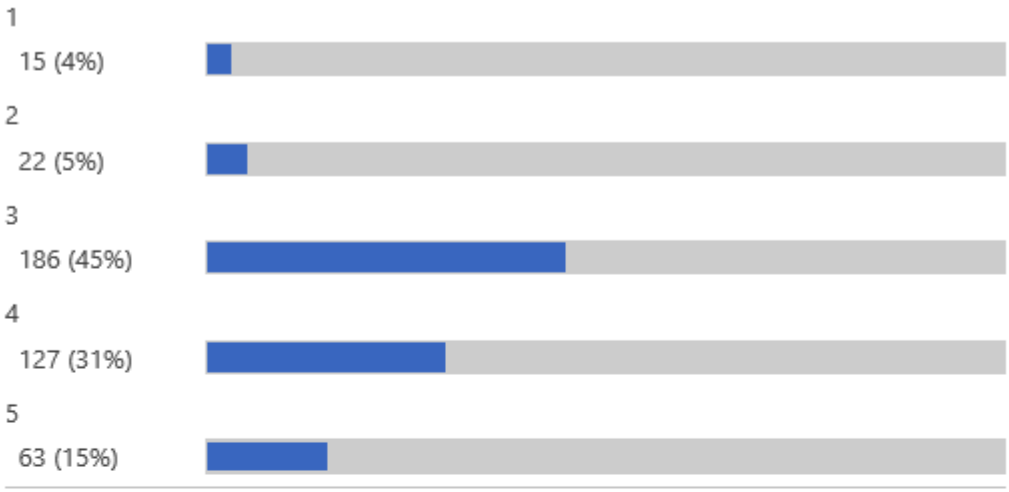
216 (52%)

Strongly Agree

72 (17%)

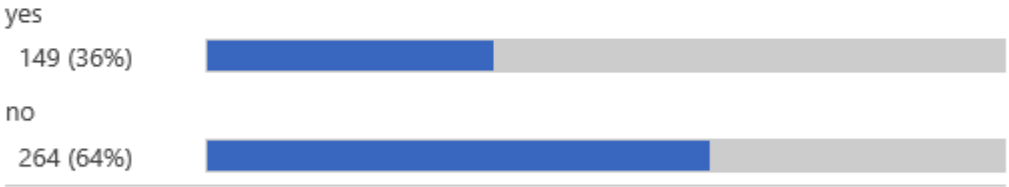
Total: 413

17. What level of computer skill do you possess? 1 (basic) to 5 (expert)



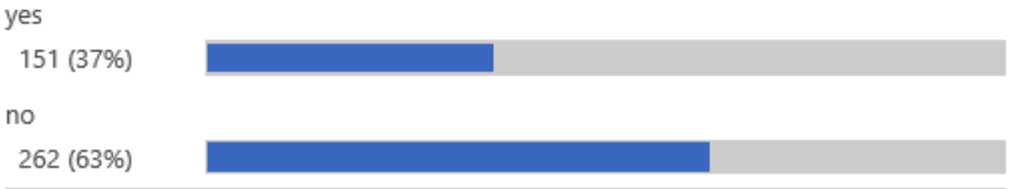
Total: 413

18. Do you have any Operational Technology (OT) background/skills?



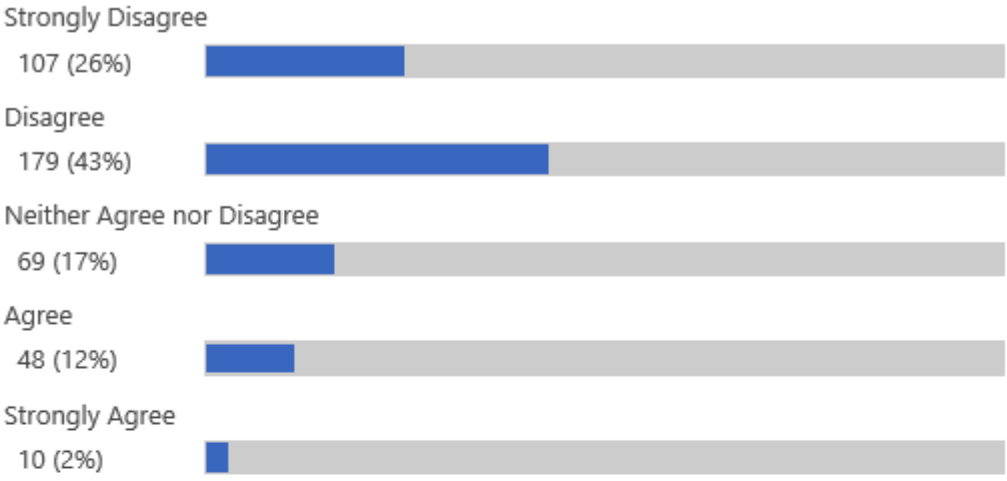
Total: 413

19. Are you aware of the Operational Technology cybersecurity standard for OT?

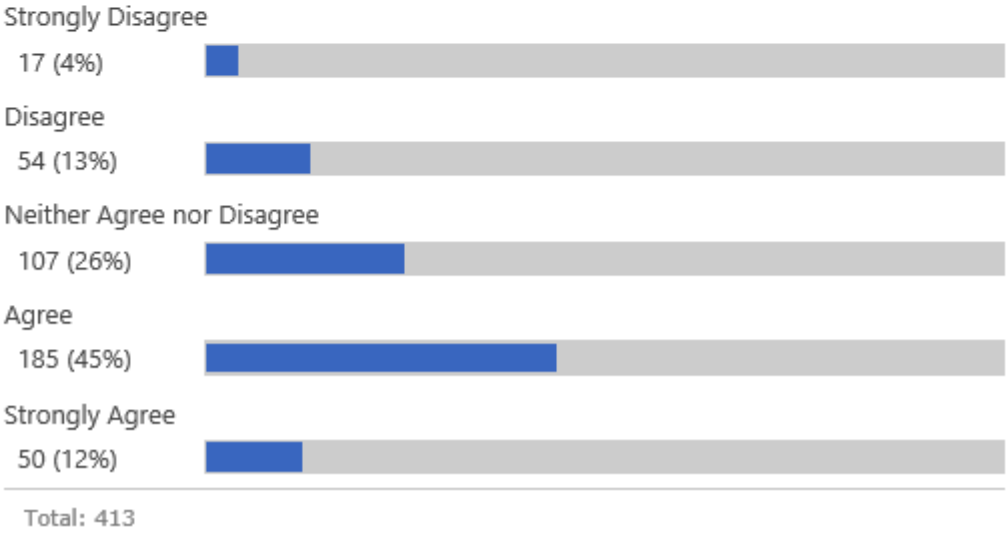


Total: 413

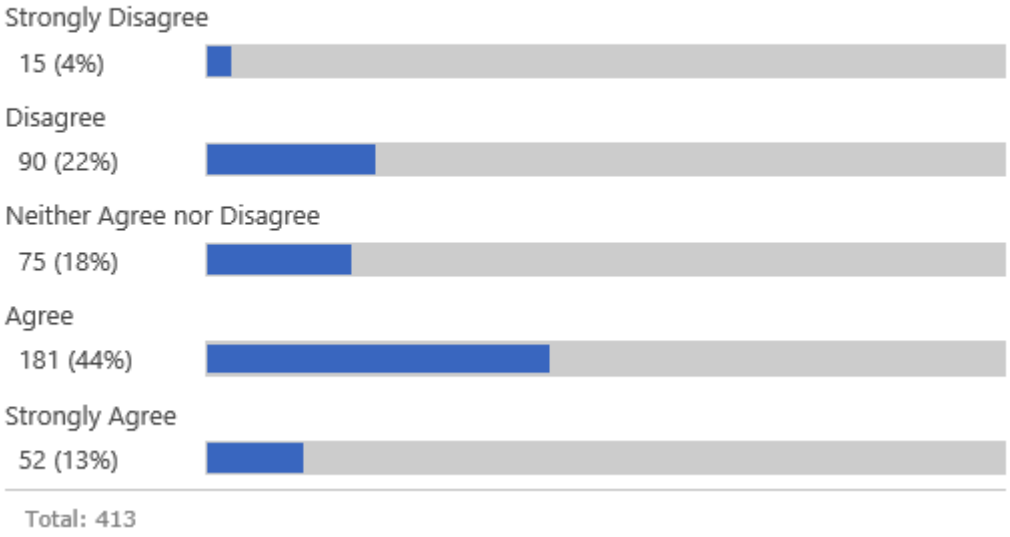
20. I am annoyed when prompted to insert a stronger password



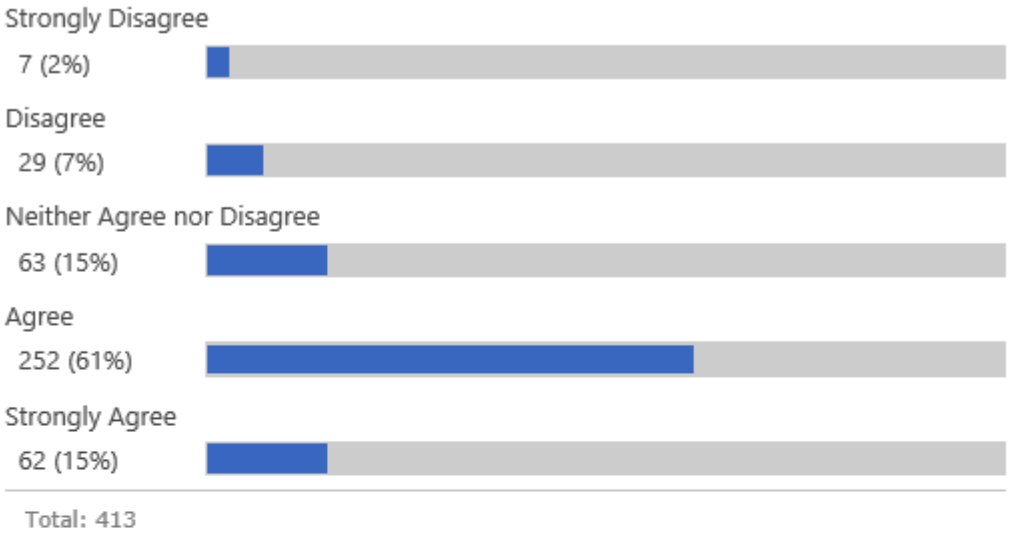
21. Eskom organisational culture embraces cybersecurity risk



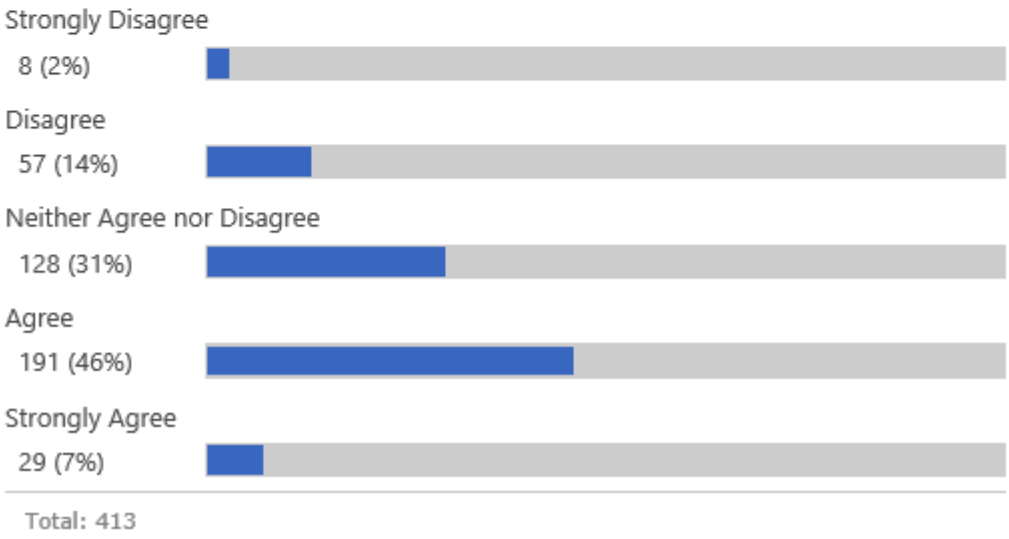
22. I scan USB/removable drives before using them



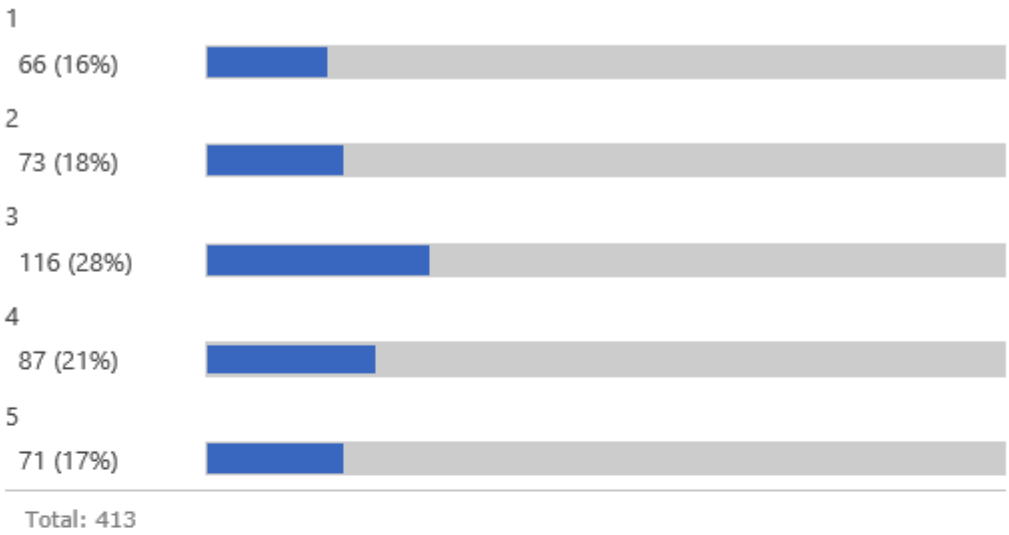
23. I read cybersecurity awareness messages/articles/media



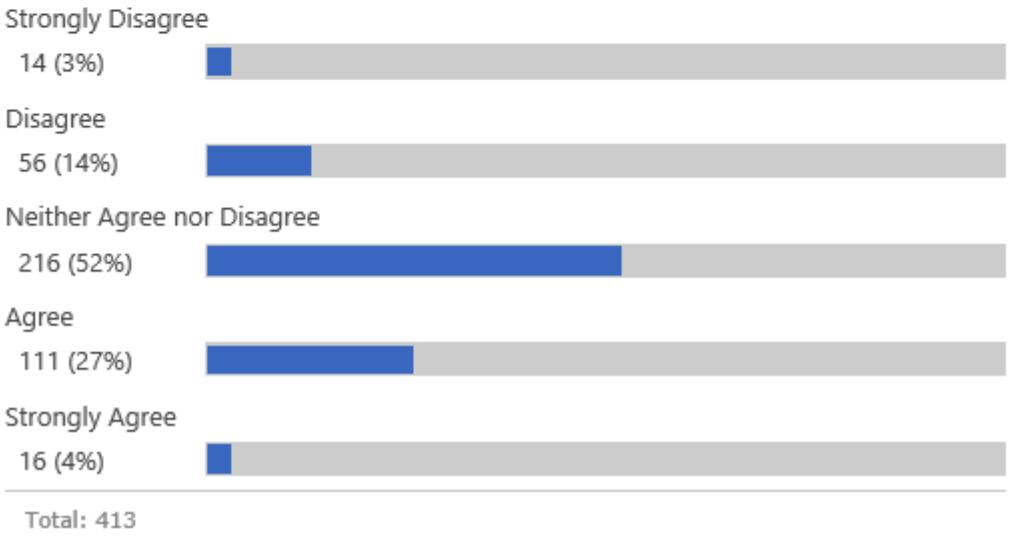
24. I share this insight (from previous question)



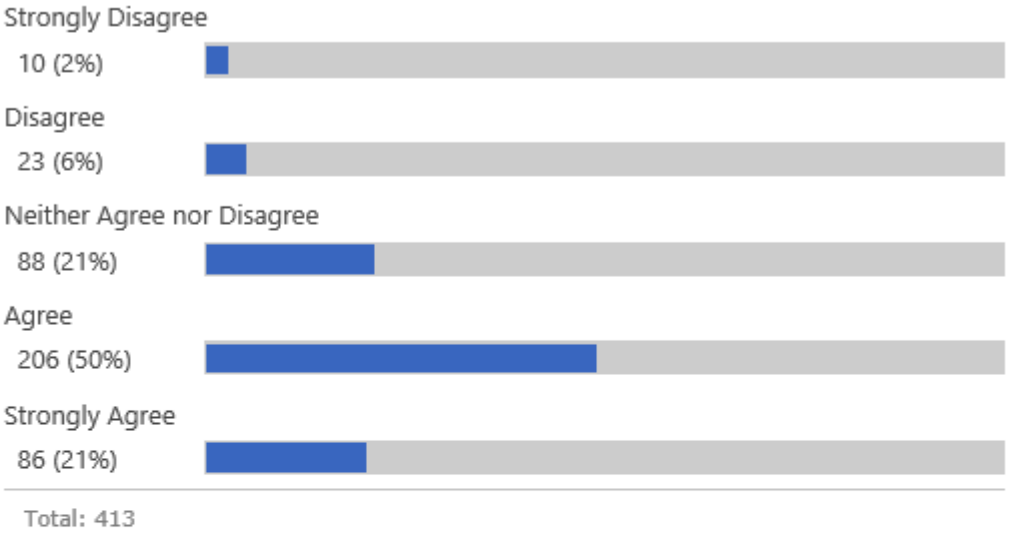
25. I report cybersecurity vulnerabilities: 1 (never) to 5 (All of the time)



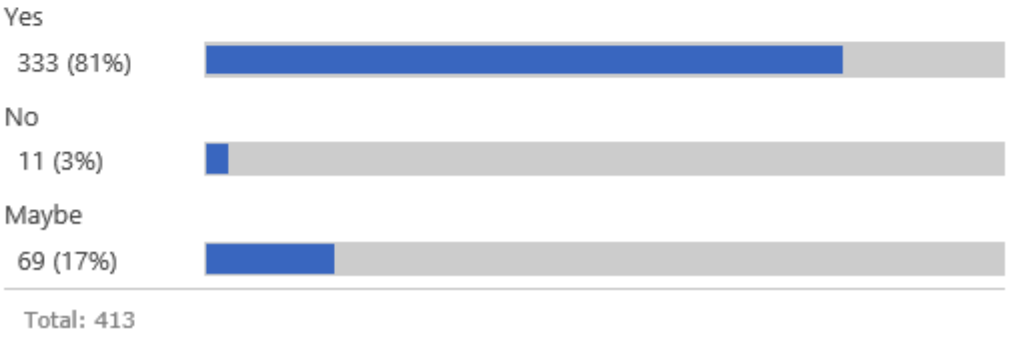
26. Eskom has good training and awareness on cybersecurity



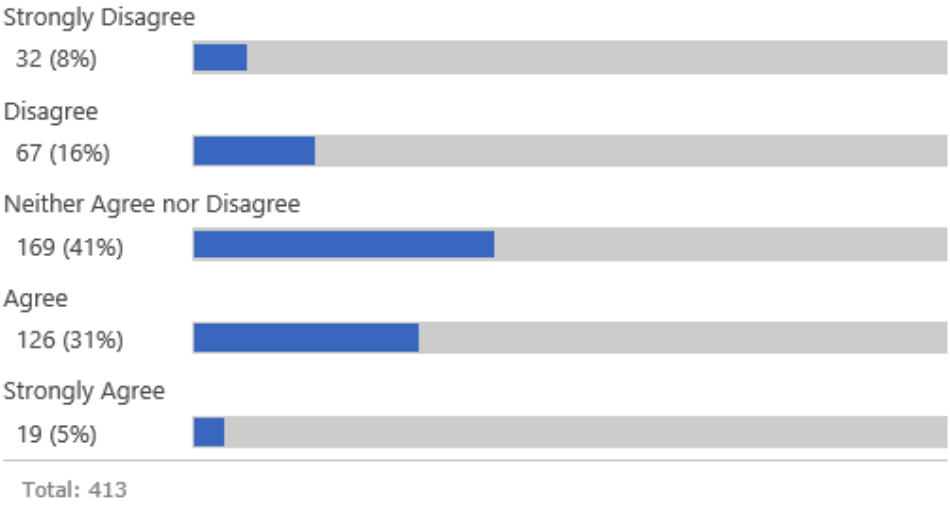
27. Eskom is vulnerable to cyber attacks



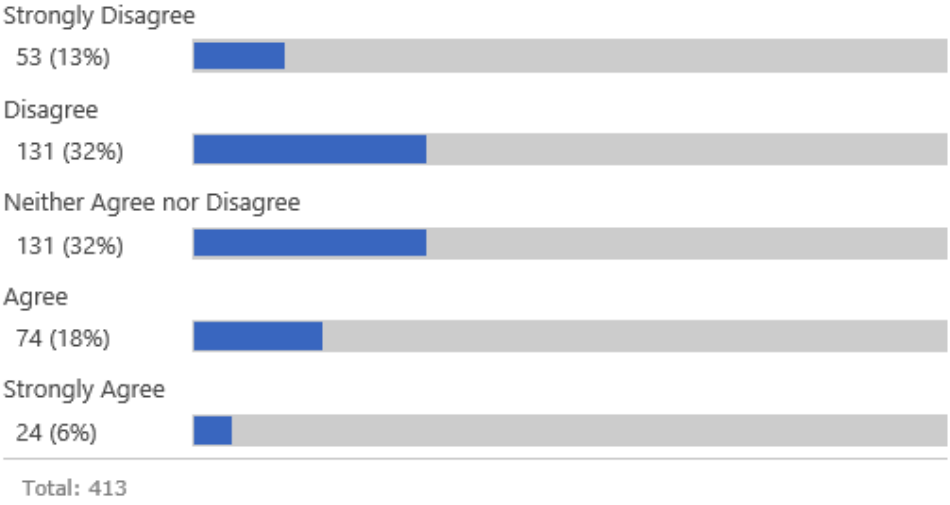
28. Do you believe that cybersecurity is your responsibility?



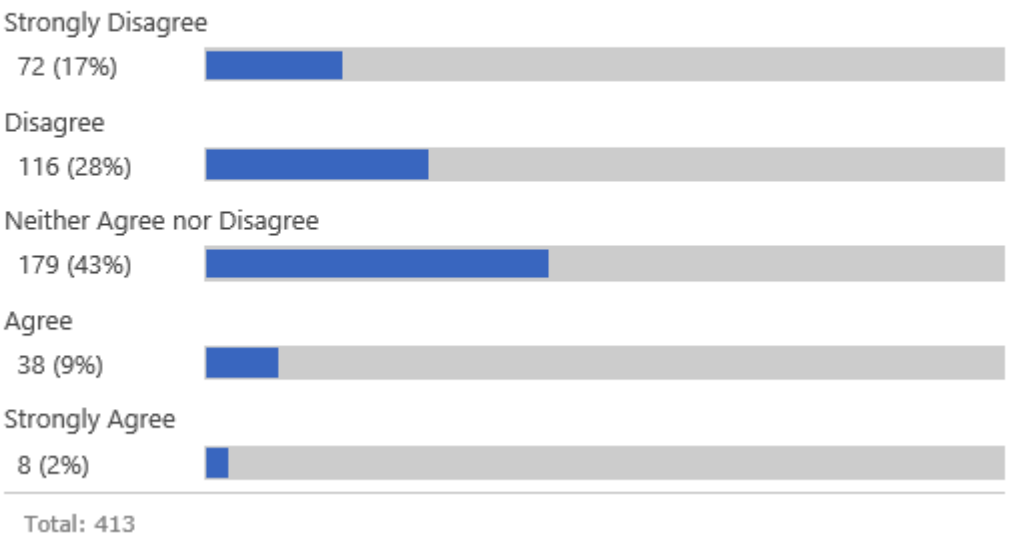
29. I trust an Eskom employee from corporate to perform assessments on my plant control systems



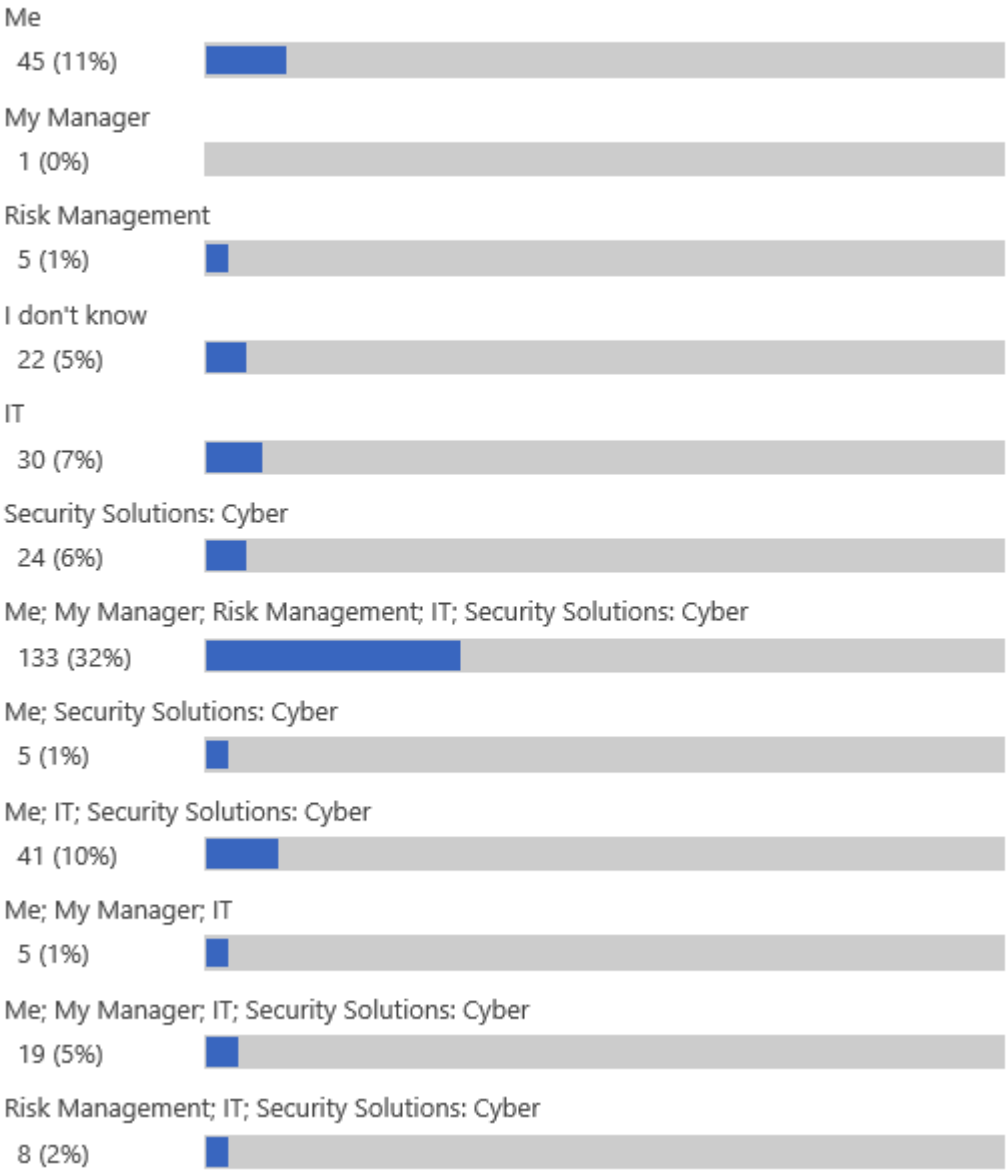
30. Cybersecurity is a topic of discussion in management meetings



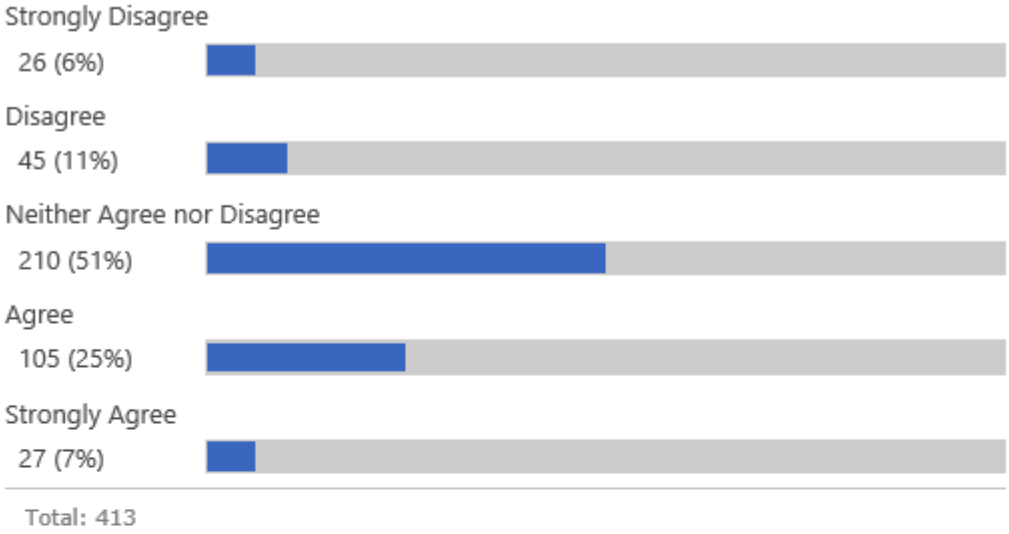
31. My department budgets for cybersecurity



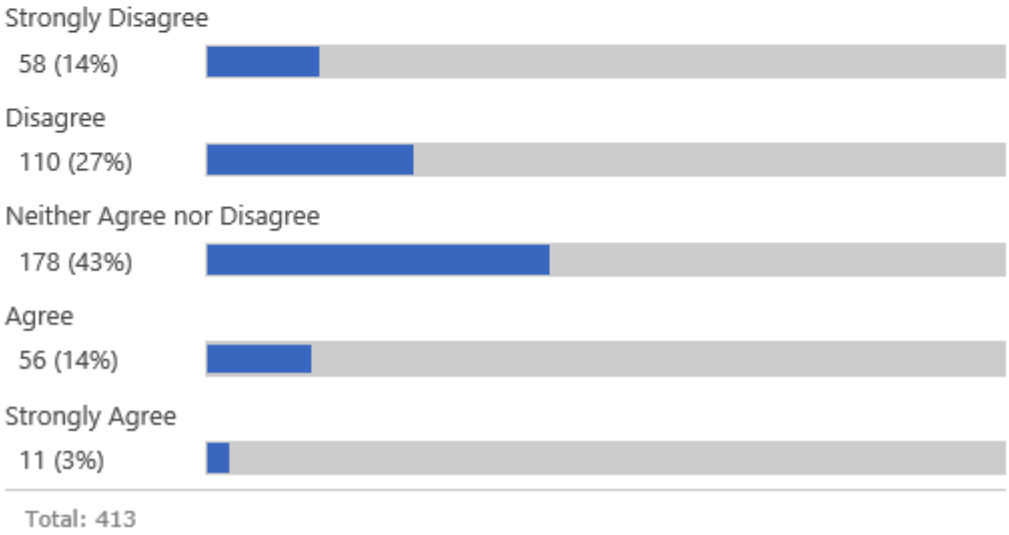
32. Who is responsible for cybersecurity in Eskom? (can choose more than one)



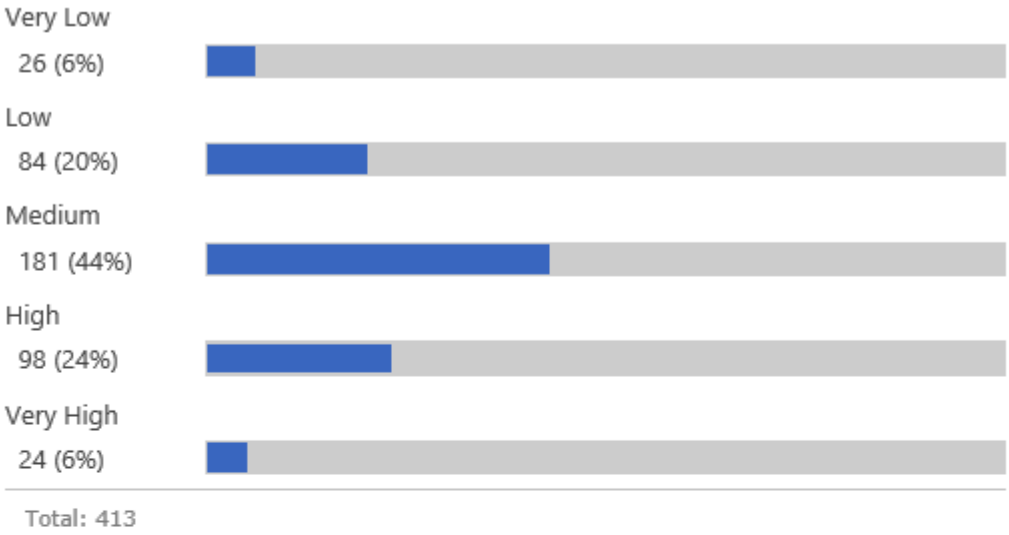
33. My manager allows me to attend cybersecurity training



34. ESKOM is ahead of Technology advancement and digitisation

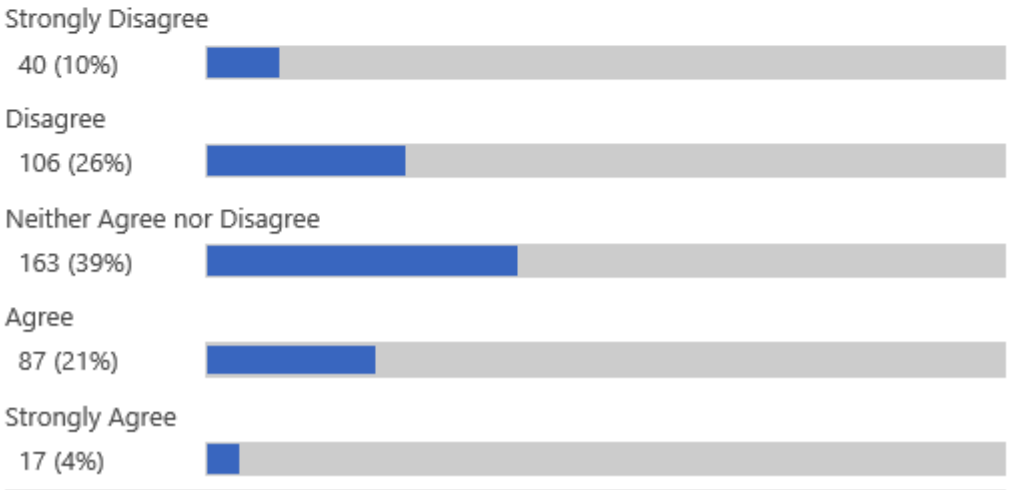


35. Rate the level of leadership commitment to protect Eskom against Cyber attack



Total: 413

36. My department assesses for cyber risk



Total: 413

37. If you approached your manager with a potential cyber risk would he/she: (can select more than one option)

Ask you to log a call

136 (33%)

Tell you he is not an IT person

11 (3%)

Not be interested

14 (3%)

Tell you to follow the risk process

60 (15%)

Proactively investigate the risk with you

43 (10%)

Ask you to log a call; Tell you to follow the risk process

46 (11%)

Ask you to log a call; Proactively investigate the risk with you

25 (6%)

Tell you he is not an IT person; Not be interested

2 (0%)

Tell you to follow the risk process; Proactively investigate the risk with you

14 (3%)

Ask you to log a call; Tell you to follow the risk process; Proactively investigate the risk with you

37 (9%)

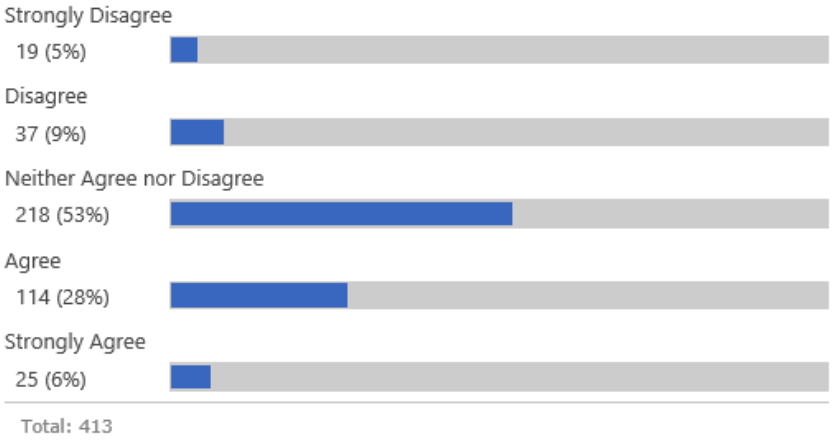
Tell you he is not an IT person; Tell you to follow the risk process

2 (0%)

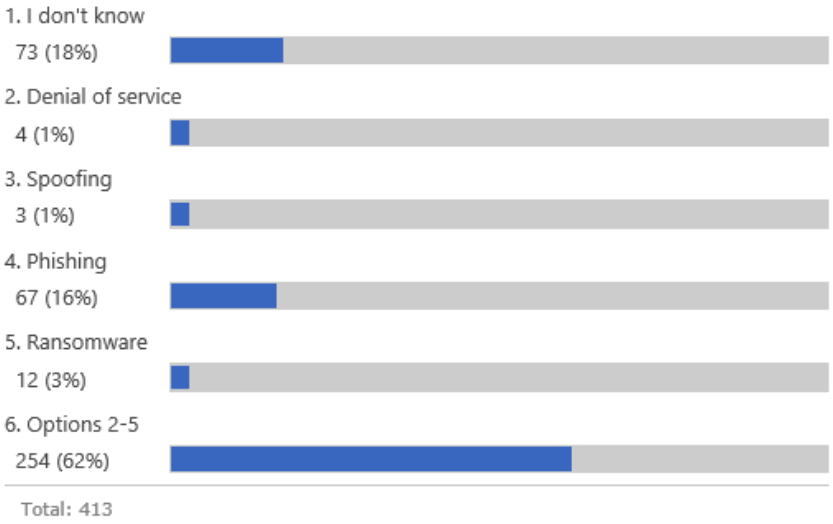
Ask you to log a call; Tell you he is not an IT person; Not be interested; Tell you to follow the risk process

2 (0%)

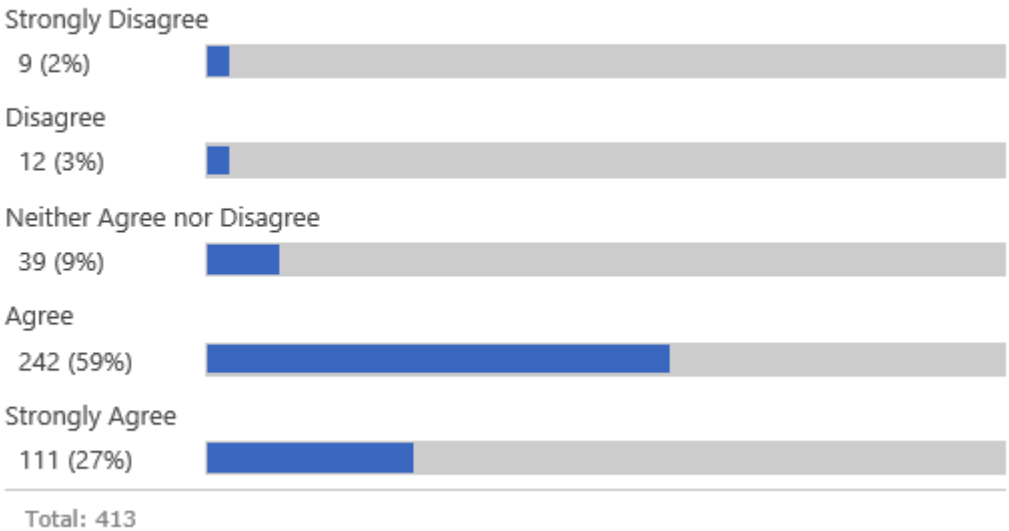
38. Senior management supports me in protecting Eskom's infrastructure by investigating cyber risks that I report



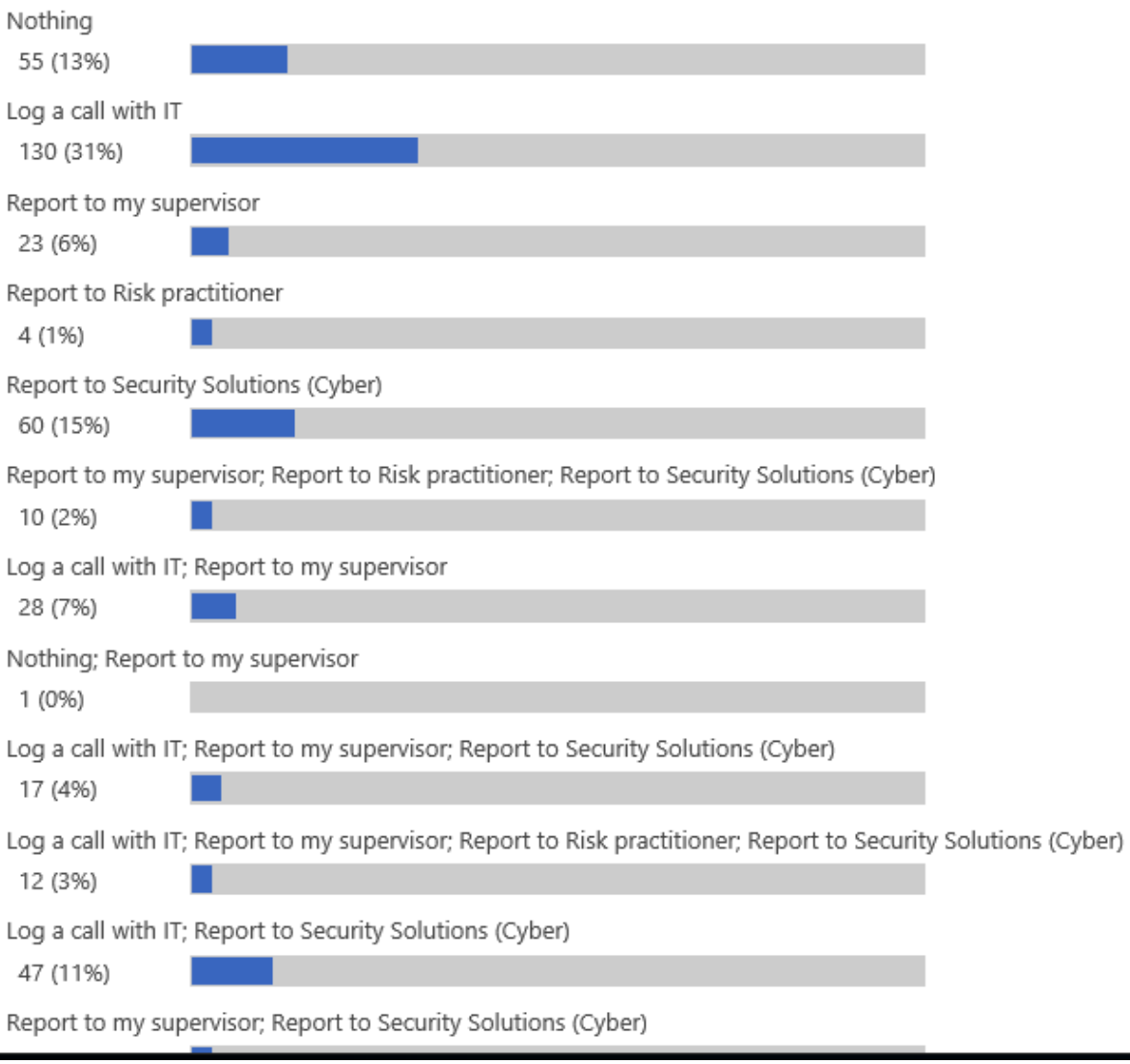
39. What kind of cyber attack is Eskom vulnerable to?



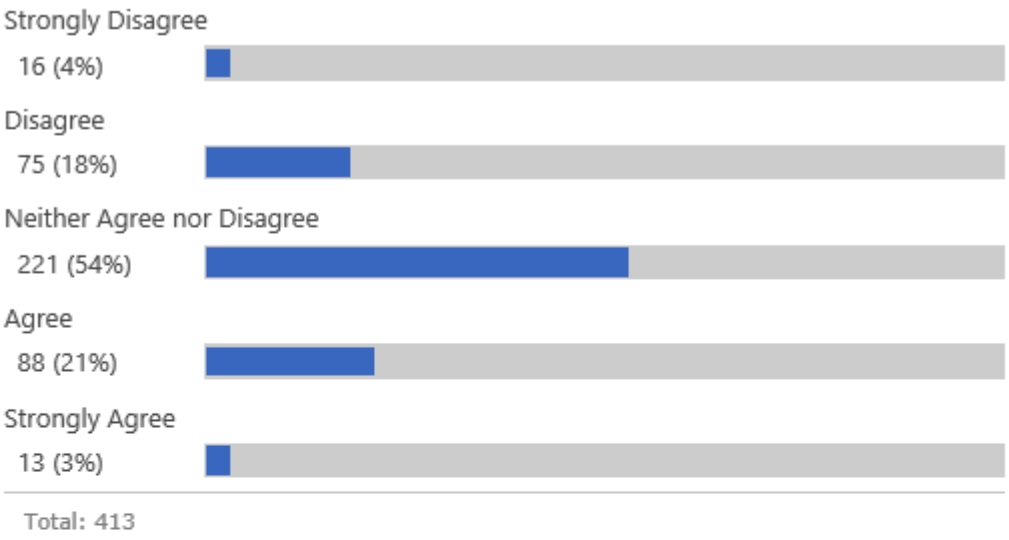
40. I recognise SCAM/ phishing emails



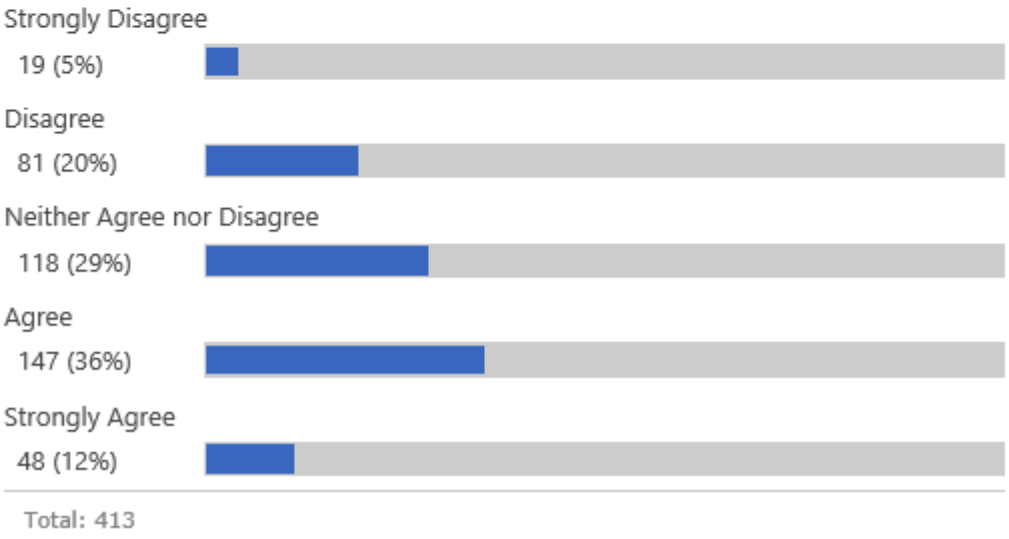
41. I do the following if I identify a cybersecurity vulnerability: (multiple selections allowed)



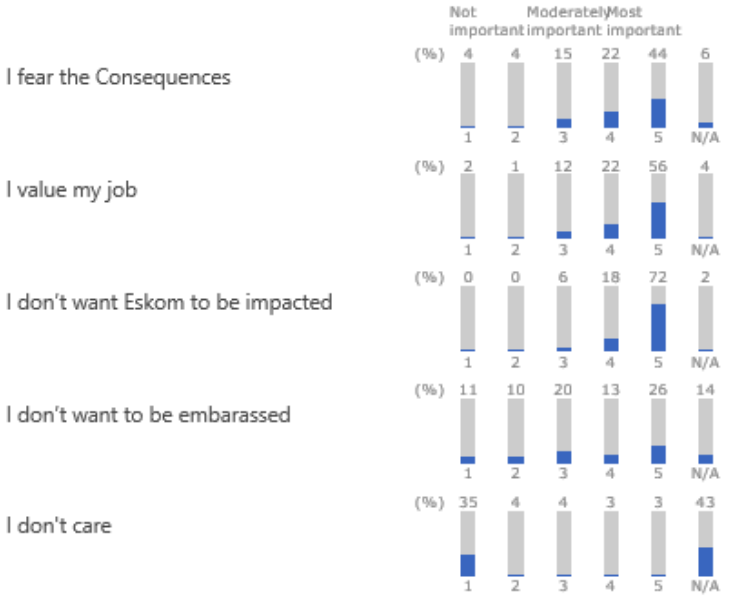
42. Eskom cybersecurity controls are fully effective



43. I have Mcafee on my computer. I am fully protected.

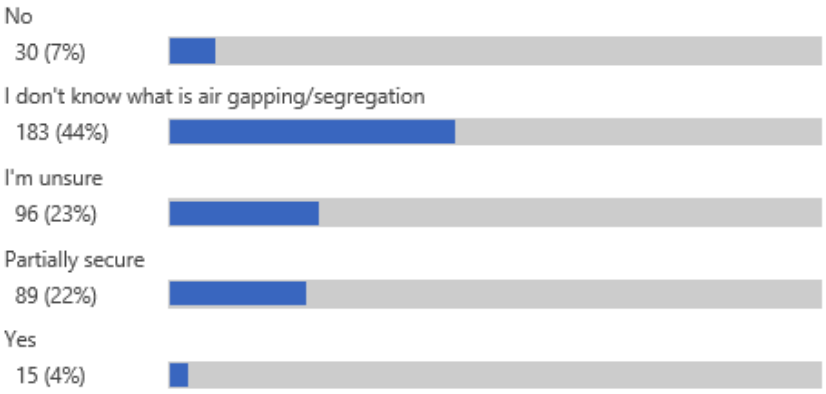


44. I comply with cybersecurity policies because:



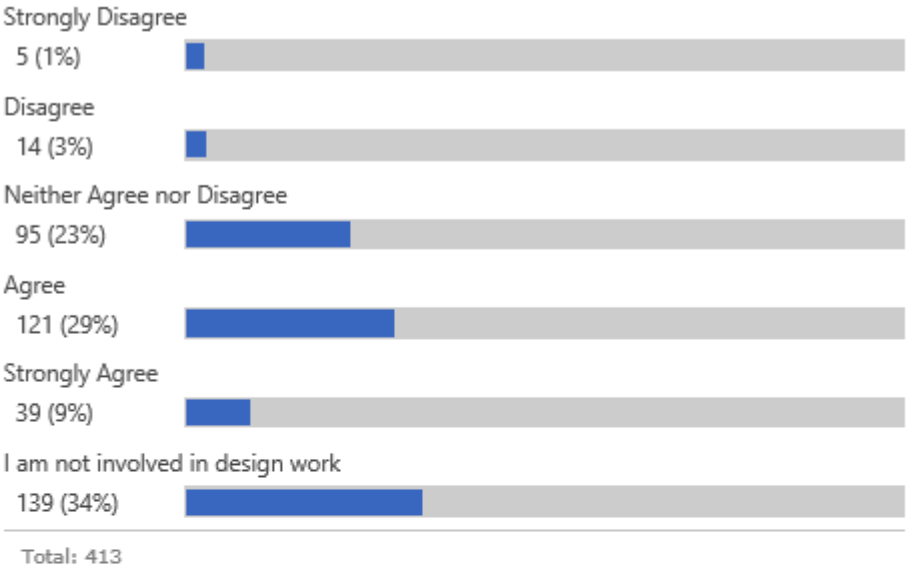
Total: 413

45. Is network segregation/air gapping an OT network sufficient protection of an Industrial Control System (ICS)?

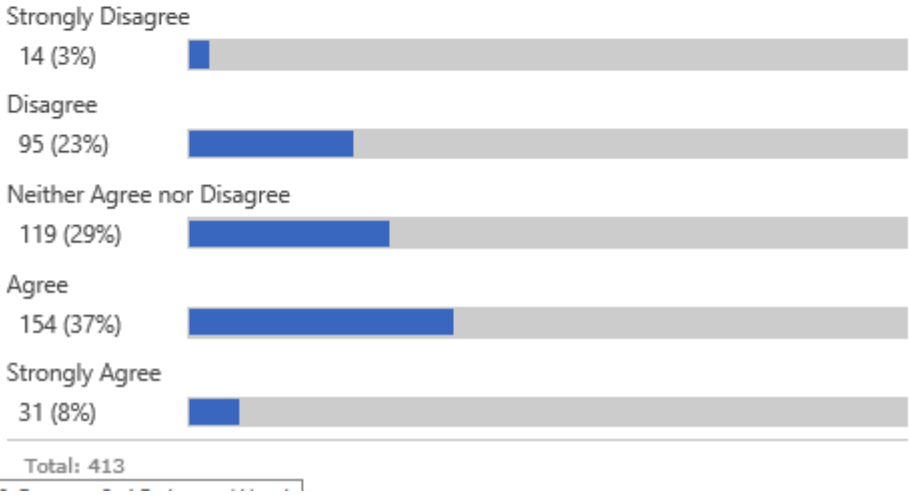


Total: 413

46. I ensure security is embedded in designs I am accountable for



47. I classify all my documents and information (Controlled disclosure, confidential,.....)



48. Cybersecurity contributes to safe plant operation

Strongly Disagree

4 (1%)

Disagree

4 (1%)

Neither Agree nor Disagree

72 (17%)

Agree

224 (54%)

Strongly Agree

109 (26%)

Total: 413

49. Do you have any antivirus/anti-malware software on your phone?

yes

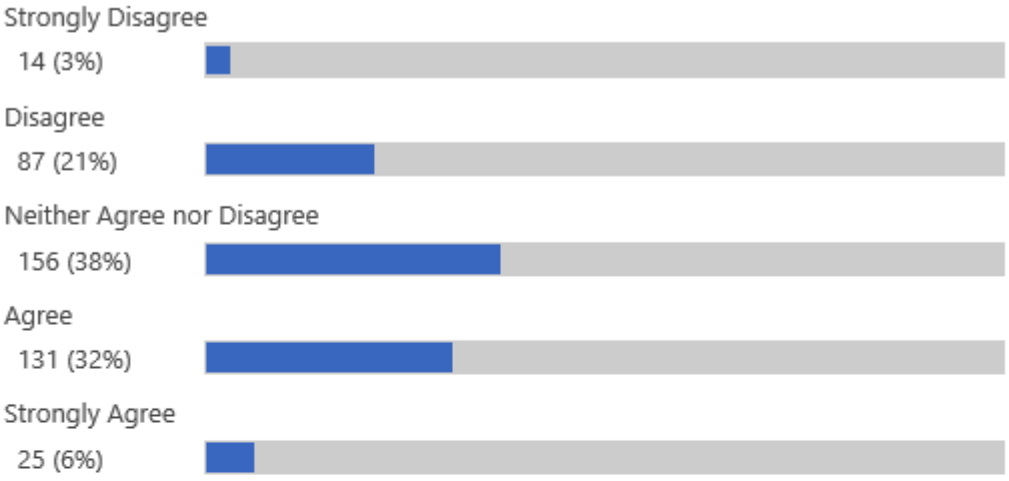
242 (59%)

no

171 (41%)

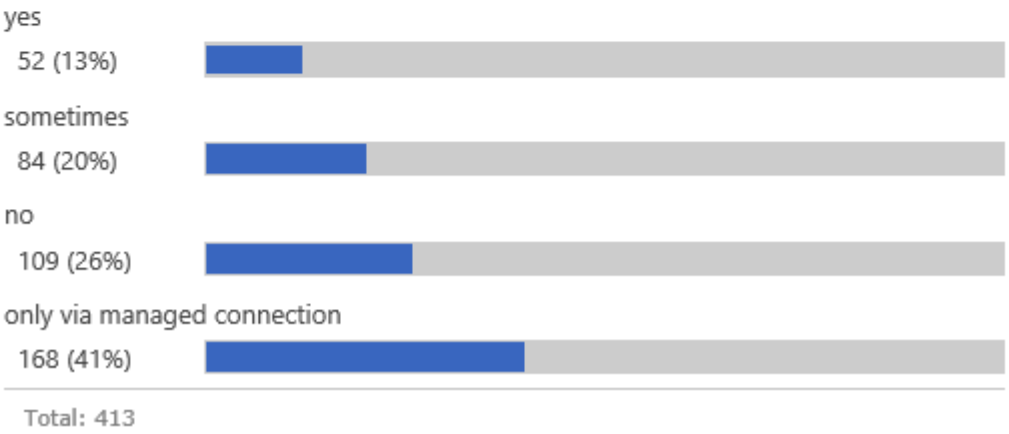
Total: 413

50. It is clear to me who has overall accountability for Cybersecurity in Eskom



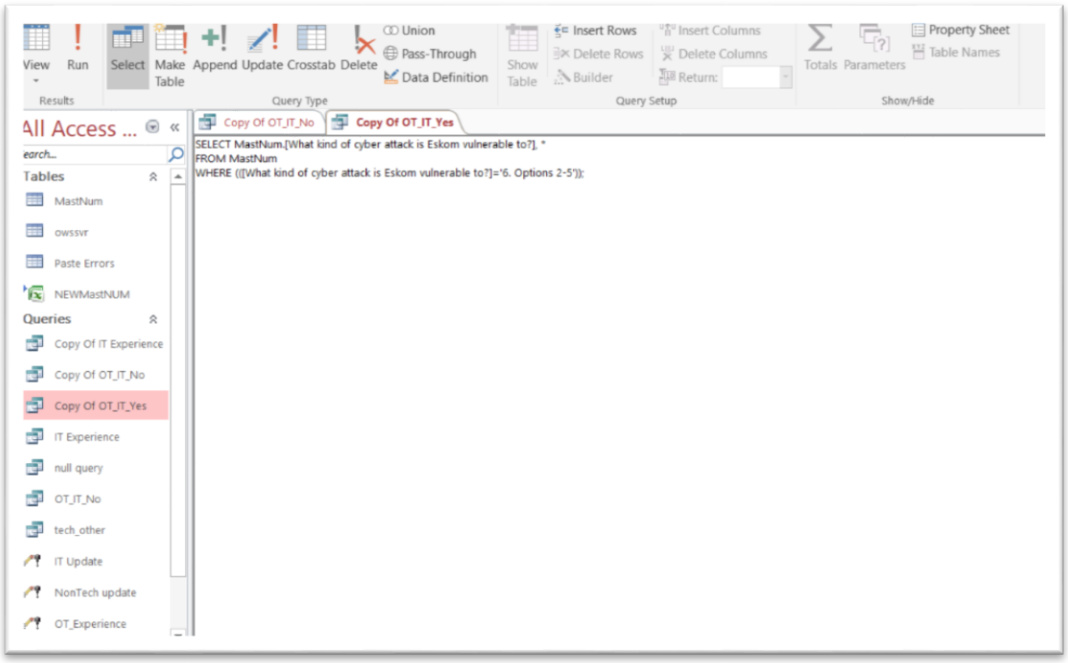
Total: 413

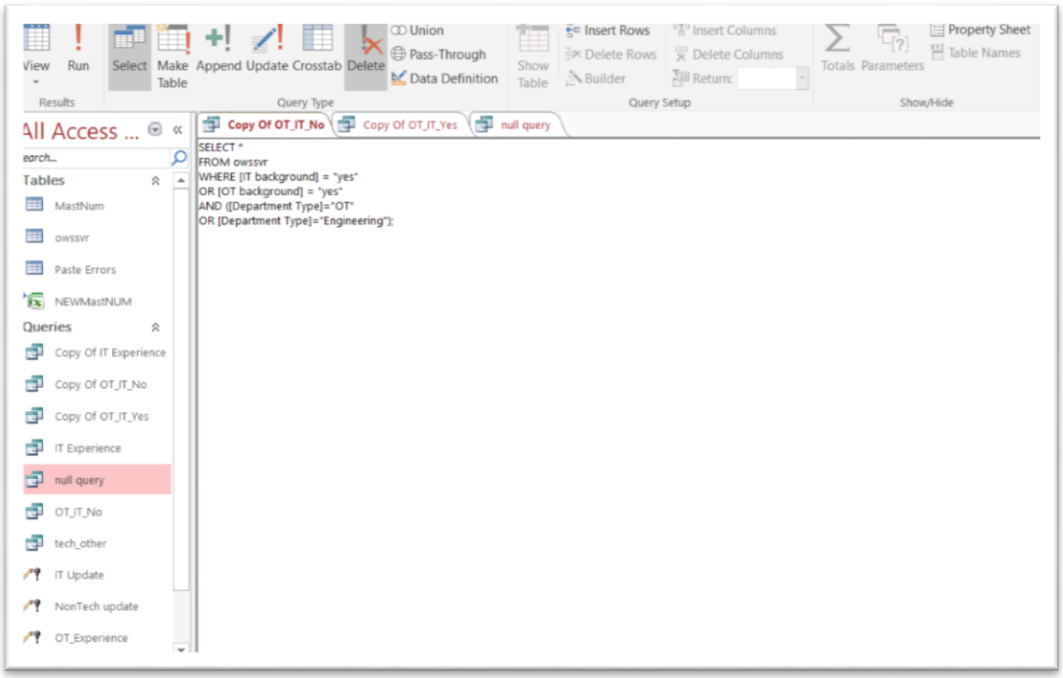
51. External service providers have remote access to Eskom Industrial control network

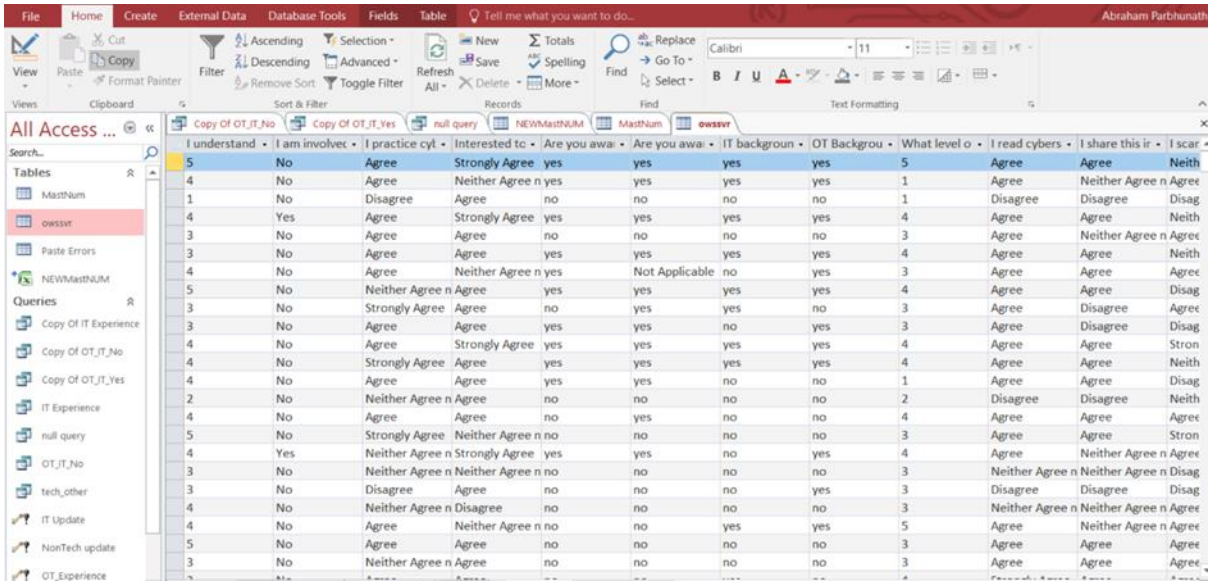


Total: 413

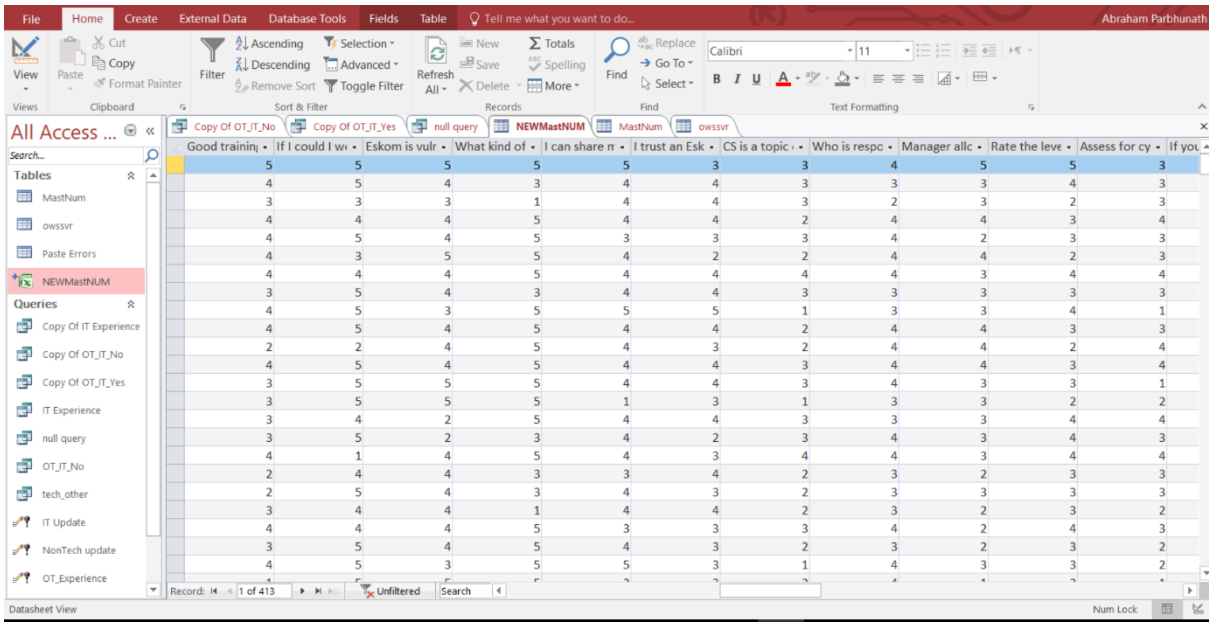
8.5 MS Access queries and data clean-up (sample)





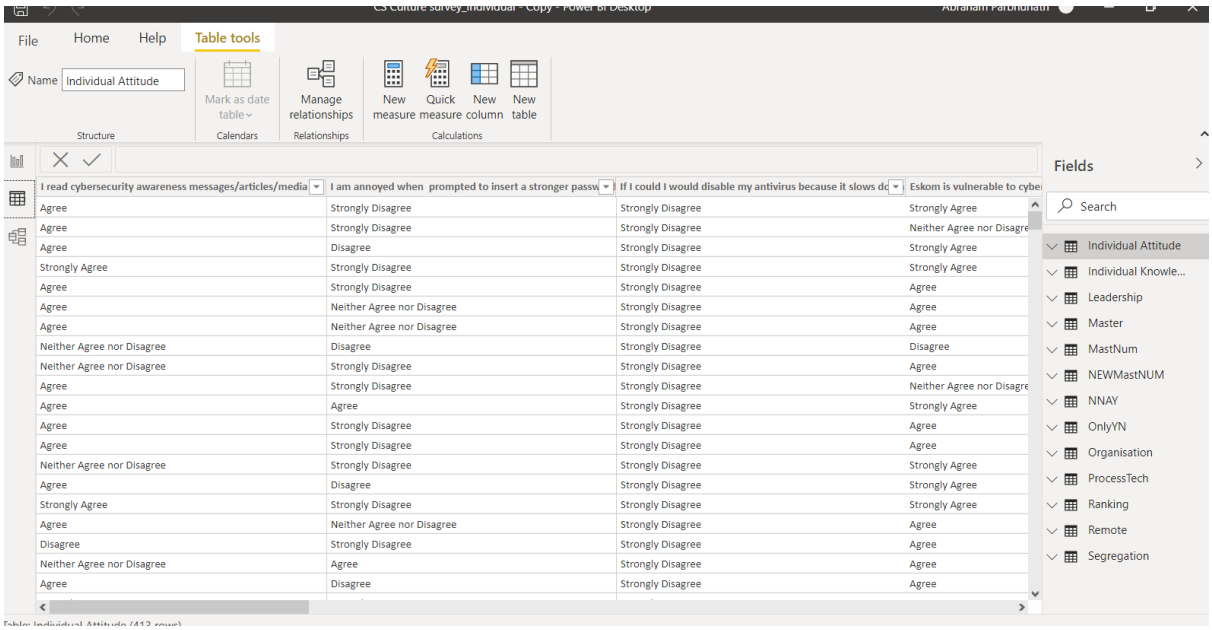


I understand	I am involvec	I practice cyt	Interested to	Are you awa	Are you awa	IT backgroun	OT Backgrou	What level o	I read cybers	I share this ir	I scar
5	No	Agree	Strongly Agree	yes	yes	yes	yes	5	Agree	Agree	Neith
4	No	Agree	Neither Agree n	yes	yes	yes	yes	1	Agree	Neither Agree n	Agree
1	No	Disagree	Agree	no	no	no	no	1	Disagree	Disagree	Disag
4	Yes	Agree	Strongly Agree	yes	yes	yes	yes	4	Agree	Agree	Neith
3	No	Agree	Agree	no	no	no	no	3	Agree	Neither Agree n	Agree
3	No	Agree	Agree	yes	yes	yes	yes	4	Agree	Agree	Neith
4	No	Agree	Neither Agree n	yes	Not Applicable	no	yes	3	Agree	Agree	Agree
5	No	Neither Agree n	Agree	yes	yes	yes	yes	4	Agree	Agree	Disag
3	No	Strongly Agree	Agree	no	yes	yes	no	3	Agree	Disagree	Agree
3	No	Agree	Agree	yes	yes	no	yes	3	Agree	Disagree	Disag
4	No	Agree	Strongly Agree	yes	yes	yes	yes	4	Agree	Agree	Stron
4	No	Strongly Agree	Agree	yes	yes	yes	yes	4	Agree	Agree	Neith
4	No	Agree	Agree	yes	yes	no	no	1	Agree	Agree	Disag
2	No	Neither Agree n	Agree	no	no	no	no	2	Disagree	Disagree	Neith
4	No	Agree	Agree	no	yes	no	no	4	Agree	Agree	Agree
5	No	Strongly Agree	Neither Agree n	no	no	no	no	3	Agree	Agree	Stron
4	Yes	Neither Agree n	Strongly Agree	yes	yes	no	yes	4	Agree	Neither Agree n	Agree
3	No	Neither Agree n	Neither Agree n	no	no	no	no	3	Neither Agree n	Neither Agree n	Disag
3	No	Disagree	Agree	no	no	no	yes	3	Disagree	Disagree	Disag
4	No	Neither Agree n	Disagree	no	no	no	no	3	Neither Agree n	Neither Agree n	Agree
4	No	Agree	Neither Agree n	no	no	yes	yes	5	Agree	Neither Agree n	Agree
5	No	Agree	Agree	no	no	no	no	3	Agree	Agree	Agree
3	No	Neither Agree n	Agree	no	no	no	no	3	Agree	Agree	Agree

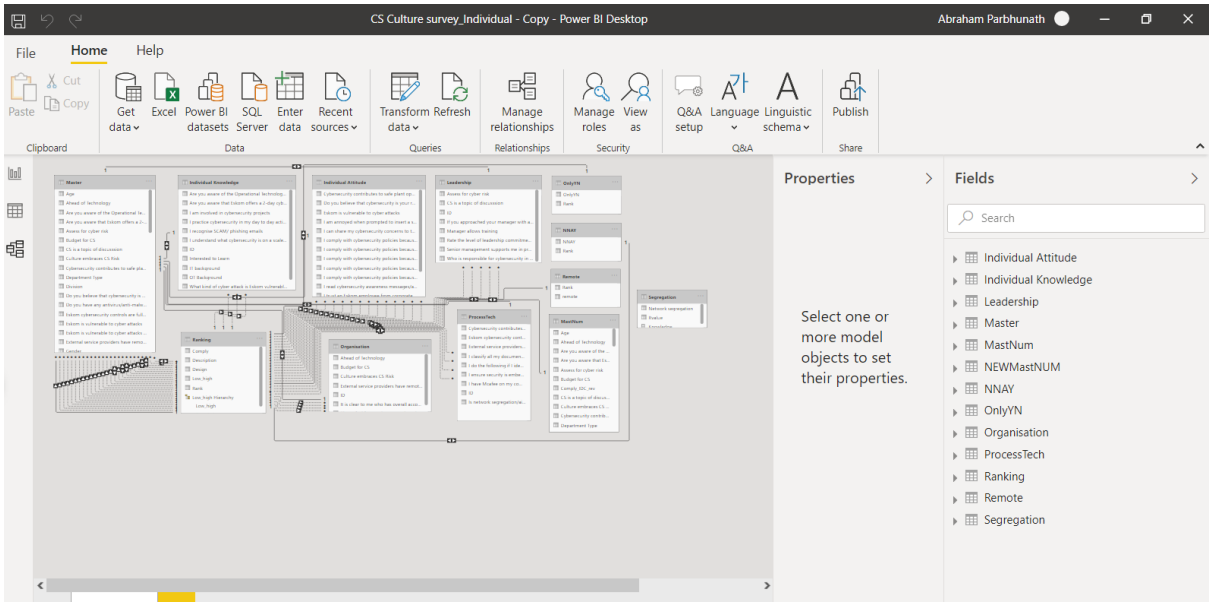


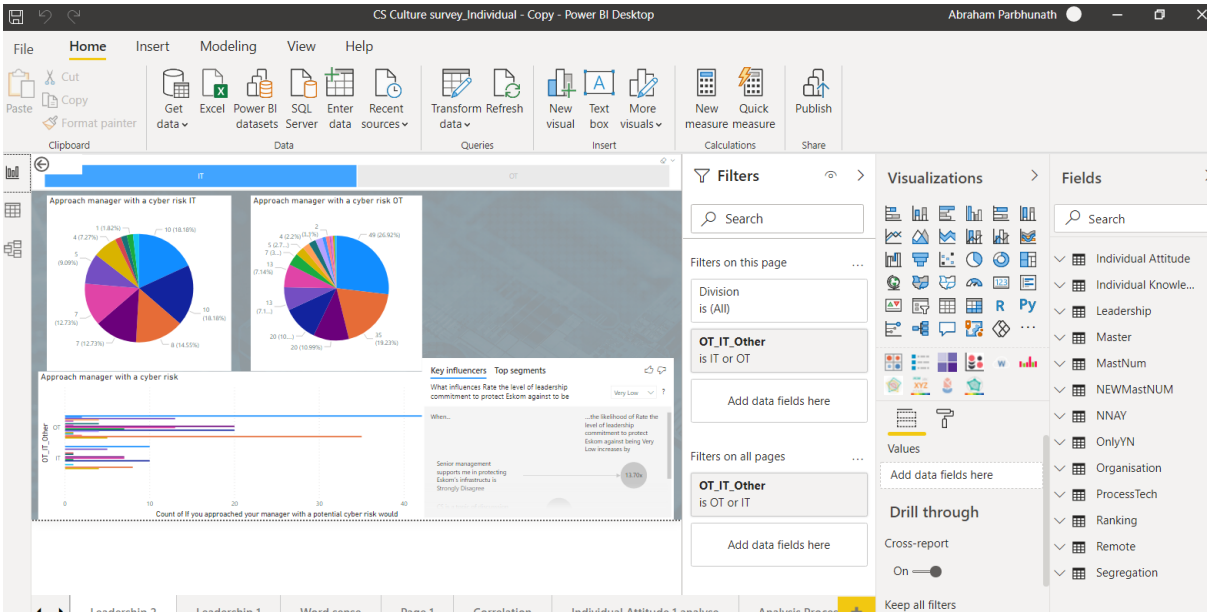
Good trainin	If I could I wi	Eskom is vulr	What kind of	I can share m	I trust an Esk	CS is a topic	Who is respc	Manager allc	Rate the leve	Assess for cy	If you
5	5	5	5	5	3	3	4	5	5	3	
4	5	4	3	4	4	3	3	3	4	3	
3	3	3	1	4	4	3	2	3	2	3	
4	4	4	5	4	4	2	4	4	3	4	
4	5	4	5	3	3	3	4	2	3	3	
4	3	5	5	4	2	2	4	4	2	3	
4	4	4	5	4	4	4	4	3	4	4	
3	5	4	3	4	4	3	3	3	3	3	
4	5	3	5	5	5	1	3	3	4	1	
4	5	4	5	4	4	2	4	4	3	3	
2	2	4	5	4	3	2	4	4	2	4	
4	5	4	5	4	4	3	4	4	3	4	
3	5	5	5	4	4	3	4	3	3	1	
3	5	5	5	1	3	1	3	3	2	2	
3	4	2	5	4	4	3	3	3	4	4	
3	5	2	3	4	2	3	4	3	4	3	
4	1	4	5	4	3	4	4	3	4	4	
2	4	4	3	3	4	2	3	2	3	3	
2	5	4	3	4	3	2	3	3	3	3	
3	4	4	1	4	4	2	3	2	3	2	
4	4	4	5	3	3	3	4	2	4	3	
3	5	4	5	4	3	2	3	2	3	2	
4	5	3	5	5	3	1	4	3	3	2	

8.6 Power BI



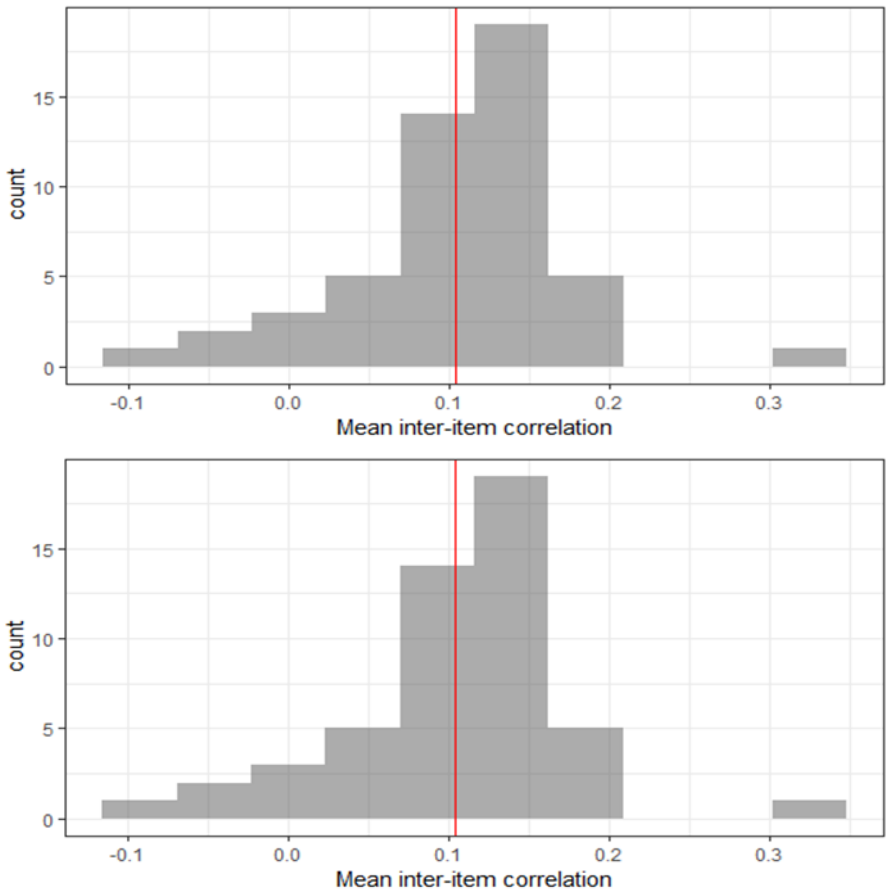
I read cybersecurity awareness messages/articles/media	I am annoyed when prompted to insert a stronger passw	If I could I would disable my antivirus because it slows dc	Eskom is vulnerable to cybe
Agree	Strongly Disagree	Strongly Disagree	Strongly Agree
Agree	Strongly Disagree	Strongly Disagree	Neither Agree nor Disagre
Agree	Disagree	Strongly Disagree	Strongly Agree
Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree
Agree	Strongly Disagree	Strongly Disagree	Agree
Agree	Neither Agree nor Disagree	Strongly Disagree	Agree
Agree	Neither Agree nor Disagree	Strongly Disagree	Agree
Neither Agree nor Disagree	Disagree	Strongly Disagree	Disagree
Neither Agree nor Disagree	Strongly Disagree	Strongly Disagree	Agree
Agree	Strongly Disagree	Strongly Disagree	Neither Agree nor Disagre
Agree	Agree	Strongly Disagree	Strongly Agree
Agree	Strongly Disagree	Strongly Disagree	Agree
Agree	Strongly Disagree	Strongly Disagree	Agree
Neither Agree nor Disagree	Strongly Disagree	Strongly Disagree	Strongly Agree
Agree	Disagree	Strongly Disagree	Strongly Agree
Strongly Agree	Strongly Disagree	Strongly Disagree	Strongly Agree
Agree	Neither Agree nor Disagree	Strongly Disagree	Agree
Disagree	Strongly Disagree	Strongly Disagree	Agree
Neither Agree nor Disagree	Agree	Strongly Disagree	Agree
Agree	Disagree	Strongly Disagree	Agree




CS Culture survey_Individual - Copy - Power BI Desktop
Abraham Parbhunath
File
Home
Insert
Modeling
View
Help
Paste
Cut
Copy
Format painter
Clipboard
Get data
Excel
Power BI datasets
SQL Server
Enter data
Recent sources
Data
Transform data
Refresh
Queries
New visual
Text box
More visuals
Insert
New measure
Quick measure
Calculations
Publish
Share
IT
OT
Approach manager with a cyber risk IT
Approach manager with a cyber risk OT
Approach manager with a cyber risk
OT_IT_Other
Count of If you approached your manager with a potential cyber risk would
Key influencers
Top segments
What influences Rate the level of leadership commitment to protect Eskom against to be
Filters
Search
Filters on this page
Division
is (All)
OT_IT_Other
is IT or OT
Add data fields here
Filters on all pages
OT_IT_Other
is OT or IT
Add data fields here
Visualizations
Values
Add data fields here
Drill through
Cross-report
On
Keep all filters
Fields
Search
Individual Attitude
Individual Knowle...
Leadership
Master
MastNum
NEWMastNUM
NNAY
OnlyYN
Organisation
ProcessTech
Ranking
Remote
Segregation

8.7 Reliability Statistics

This was based on DrSimonj's blog [98]



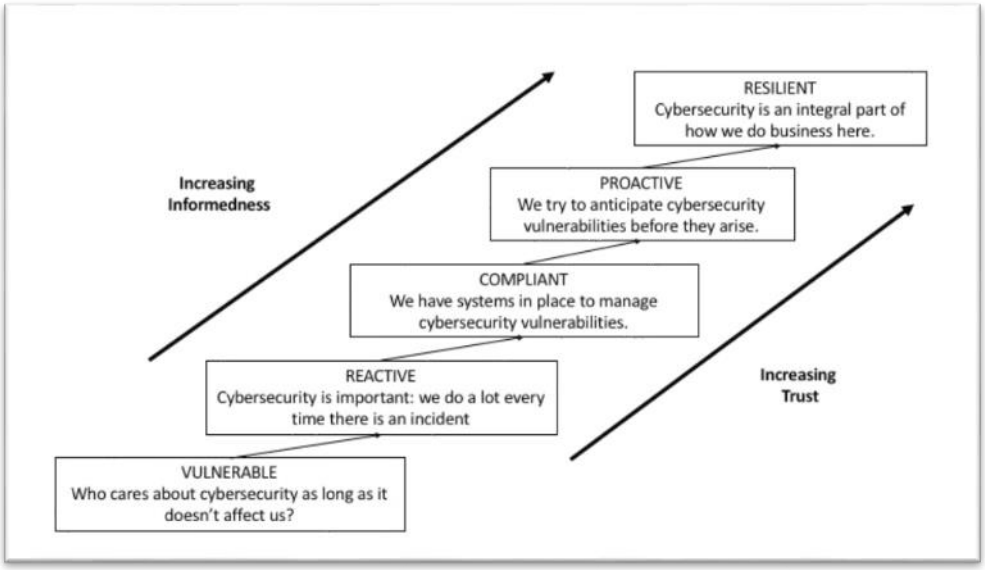

```
library(readxl)
Book1 <- read_excel("C:/Users/NkabinMP/Desktop/work -ducument/Rosherville/2020-2021 work/Abraham Parbhunath/Book1.xlsx",
           sheet = "Sheet1")

attach(Book1)

#https://drsimonj.svbtle.com/how-to-calculate-internal-consistency
#https://www.r-bloggers.com/2016/08/five-ways-to-calculate-internal-consistency/


##############################################################################################################################################

# Average inter-item correlation

#The average inter-item correlation is any easy place to start.
#To calculate this statistic, we need the correlations between all items,
#and then to average them. Let's use my corrr package to get these correlations
#as follows (no bias here!):

library(corrr)
library(dplyr)
Book1%>% correlate()
```

```
#Because the diagonal is already set to NA, we can obtain the average correlation of each
#item with all others by computing the means for each column (excluding the rowname column):

inter_item <- Book1 %>% correlate() %>% select(-rowname) %>% colMeans(na.rm = TRUE)
inter_item

#To obtain the overall average inter-item correlation, we calculate the mean() of these values:

mean(inter_item)
#0.1041935

library(corrr)
library(dplyr)
library(ggplot2)


#However, with these values, we can explore a range of attributes about the relationships between the items.
#For example, we can visualise them in a histogram and highlight the mean as follows:

data.frame(inter_item) %>%
  ggplot(aes(x = inter_item)) +
  geom_histogram(bins = 10, alpha = .5) +
  geom_vline(xintercept = mean(inter_item), color = "red") +
  xlab("Mean inter-item correlation") +
  theme_bw()
#########################################################################################################
#################################################


#Average item-total correlation

#We can investigate the average item-total correlation in a similar way to the inter-item correlations.
#The first thing we need to do is calculate the total score.
#Let's say that a person's score is the mean of their responses to all ten items:


Book1$score <- rowMeans(Book1)
head(Book1)

#Now, we'll correlate() everything again, but this time focus() on the correlations of the score with the items:

item_total <- Book1 %>% correlate() %>% focus(score)
item_total

#Again, we can calculate their mean as

mean(item_total$score)
#> [1] 0.3346003


item_total %>%
  ggplot(aes(x = score)) +
  geom_histogram(bins = 10, alpha = .5) +
  geom_vline(xintercept = mean(item_total$score), color = "red") +
  xlab("Mean item-total correlation") +
  theme_bw()

#########################################################################################################
```

```
##########################

#Cronbach's alpha



library(psych)


psych::alpha(Book1)

#

psych::alpha(Book1)$total$std.alpha

#0.8531356

#########################################################################################################
########################################

#Composite reliability

#The final method for calculating internal consistency that we'll cover is composite reliability.
#Where possible, my personal preference is to use this approach. Although it's not perfect, it
#takes care of many inappropriate assumptions that measures like Cronbach's alpha make. If the
#specificities interest you, I suggest reading this post.

#Composite reliability is based on the factor loadings in a confirmatory factor analysis (CFA).
#In the case of a unidimensional scale (like extraversion here), we define a one-factor CFA, and
#then use the factor loadings to compute our internal consistency estimate. I won't go into the detail,
#but we can interpret a composite reliability score similarly to any of the other metrics covered here
#(closer to one indicates better internal consistency). We'll fit our CFA model using the lavaan package as
follows:


library(lavaan)

# Define the model
items <- paste(names(Book1), collapse = "+")
model <- paste("extraversion", items, sep = "=~")
model
#> [1] "extraversion=~E1+E2+E3+E4+E5+E6+E7+E8+E9+E10"

# Fit the model
fit <- cfa(model, data = Book1)


###

library(readxl)
Book2<- read_excel("C:/Users/NkabinMP/Desktop/work -ducument/Rosherville/2020-2021 work/Abraham
Parbhunath/Book2.xlsx",
            sheet = "Sheet1")

attach(Book2)

library(lavaan)

# Define the model
items <- paste(names(Book2), collapse = "+")
```

```
model <- paste("extraversion", items, sep = "=~")
model
#> [1] "extraversion=~E1+E2+E3+E4+E5+E6+E7+E8+E9+E10+..."

# Fit the model
fit <- cfa(model, data = Book2)

#There are various ways to get to the composite reliability from this model.
#After receiving a great suggestion from Gaming Dude, a nice approach is to
#use reliability() from the semTools package as follows:

library(semTools)
reliability(fit)

#You can see that this function returns a matrix with five reliability
#estimates for our factor (including Cronbach's alpha). In this case,
#we're interested in omega, but looking across the range is always a good idea.
#A nice advantage to this function is that it will return the reliability estimates
#for all latent factors in a more complex model!

#Below is the original method I had posted, involving a "by-hand" extraction of the factor loadings
#and computation of the omega composite reliability.

sl <- standardizedSolution(fit)
sl <- sl$est.std[sl$op == "=~"]
names(sl) <- names(Book2)
sl

# Compute residual variance of each item
re <- 1 - sl^2

# Compute composite reliability
sum(sl)^2 / (sum(sl)^2 + sum(re))
```

8.8 Examples of Maturity scales


RESILIENT
Cybersecurity is an integral part of how we do business here.
PROACTIVE
We try to anticipate cybersecurity vulnerabilities before they arise.
COMPLIANT
We have systems in place to manage cybersecurity vulnerabilities.
REACTIVE
Cybersecurity is important: we do a lot every time there is an incident
VULNERABLE
Who cares about cybersecurity as long as it doesn't affect us?
Increasing Informedness
Increasing Trust