Analysis of COVID-19 Effects on Cybersecurity in South African-based Organisations

Mahima Daya

Student number: DYXMAH001

dyxmah001@myuct.ac.za

University of Cape Town

Commerce Faculty

Supervisor: Michael Kyobe

Thesis submitted for part fulfilment of the Master's Degree in Information Systems

May, 2024

DECLARATION:

1. I am presenting this dissertation in FULL/PARTIAL fulfilment of the requirements for my degree.

2. I know the meaning of plagiarism and declare that all of the work in the dissertation, save for that which is properly acknowledged, is my own.

3. I hereby grant the University of Cape Town free licence to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever of the above dissertation.

Signature: Signed by candidate Date: 23 May 2024

Abstract

The COVID-19 pandemic has significantly impacted cybersecurity practices in South African organisations across various sectors, including financial services, healthcare, retail, and technology, with vulnerabilities arising from remote work, digital infrastructure, and financial strain. This study applied Engström's Activity Theory Framework to explore the effects of the pandemic on cyber-threats, vulnerabilities, and organisational responses. The findings reveal that remote workers faced significant vulnerabilities during the pandemic, making them susceptible to phishing and social engineering attacks. The study highlights the importance of cybersecurity awareness training and education for employees in South African organisations. The economic instability of South Africa during the pandemic led to an increased appeal of cyber-threats, underscoring the need for enhanced cybersecurity strategies. The study's findings provide practical recommendations for enhancing cybersecurity strategies, including the adoption of secure remote work solutions and the development of incident response plans. The results underscore the importance of cybersecurity awareness training and education for employees. The study's methodology involved conducting 30 semi-structured interviews with South African organisations from the financial, healthcare, retail, and technology sectors, employing thematic analysis to delve into the realm of cybersecurity management practices during the pandemic. Despite its limitations, including a limited data sample and potential lack of generalisability to all South African organisations, this study contributes to the existing literature and provides valuable insights for policymakers, organisations, and cybersecurity professionals. The findings suggest that to mitigate risks, organisations should prioritise cybersecurity and invest in comprehensive cybersecurity solutions. Employee training is essential for enhancing cybersecurity awareness and preventing cyberattacks. Regulatory compliance is crucial for ensuring data privacy and security standards are met. Investments in digital infrastructure and cybersecurity education and training are also recommended to equip future professionals with the necessary skills to address emerging cyber threats. Future research should consider expanding data sources and conducting long-term analyses to gain a more comprehensive understanding of the cybersecurity challenges during and beyond the pandemic.

Keywords: COVID-19, Cybersecurity, cybersecurity awareness training, remote work, South African organisations, vulnerabilities.

Acknowledgments

I would like to begin by expressing my deepest gratitude to the Lord, who has been a constant source of guidance and support throughout my academic journey.

I am deeply thankful for the unwavering support and encouragement of my parents and aunt, which have been a constant source of inspiration throughout my academic journey.

My sincerest appreciation goes to Professor Michael Kyobe, whose exceptional supervision has been instrumental in shaping my research and ideas. His guidance, expertise, and mentorship have been invaluable in refining my arguments and improving the quality of my work. His insightful feedback, constructive criticism, and encouragement have been pivotal in helping me to achieve my goals.

I also extend my gratitude to Mike Leisegang of 'Well Spotted Editing', my editor, who has diligently reviewed and edited my dissertation. His meticulous work has greatly improved the clarity and coherence of my work, and his attention to detail and expertise have been invaluable in presenting my research in a clear and concise manner.

All these contributions have been instrumental in enabling me to complete my Master's dissertation successfully.

CONTENTS

List of Tables

List of Figures

List of Acronyms

Acronym	Meaning
ALT	Action Learning Theory
ATF	Activity Theory Framework
CEH	Certified Ethical Hacker
CEO	Chief Executive Officer
CIS	Center for Internet Security (USA)
CISM	Certified Information Security Manager
CLT	Cognitive Load Theory
COBIT	Control Objectives for Information and Related Technology
CompTIA	Computer Technology Industry Association
COVID-19	Coronavirus 2019
CVSS	Common Vulnerability Scoring System
DDoS	Distribute Denial of Service
DNS	Domain Name System
DoS	Denial of Service
DT	Deterrence Theory
EDR	Endpoint Defence and Response
ELT	Experiential Learning Theory
EPPM	Extended Parallel Process Model
FT	Fraud Theory
HTTPS	Hypertext Transfer Protocol Secure
IS	Information Security
ISC2	International Information System Security Certification Consortium
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
RAT	Routine Activity Theory
RCT	Rational Choice Theory
SA	South Africa

SCT	Social Cognitive Theory
SDT	Social Disorganisation Theory
SET	Social Exchange Theory
SIT	Social Identity Theory
SLT	Social Learning Theory
SOC	Security Operations Centre
ST	Strain Theory
STS	Social Technical Systems
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
UK	United Kingdom
US	United States
USB	Universal Serial Bus
UTAUT	Unified Theory of Acceptance and Use of Technology
VPN	Virtual Private Network

Chapter 1: Introduction

Chapter 1 provides an overview and background to provide context for the research. The research problem and justification are presented, followed by the study's research questions, objective, and its intended contribution to further research.

1.1 Background

As a result of the Coronavirus disease 2019 (COVID-19) pandemic, there have been significant changes in the way businesses operate. Amankwah-Amoah et al. (2021) emphasise the growing importance of technology in facilitating these shifts. Technology adoption played a crucial role in ensuring business continuity during the pandemic (AlShamsi et al., 2020). The outbreak exposed the digital divide between organisations that had invested in technology and those that had not (Lythreatis et al., 2022).

Organisations with pre-existing digital infrastructures were more effectively able to navigate the technology challenges caused by the pandemic (Bryant et al., 2020). However, this rapid transition to remote work and digital platforms exposed organisations to new vulnerabilities, with cybercriminals taking advantage of weaknesses in their cybersecurity strategies (Saleous et al., 2021). Therefore, Chigada and Madzinga (2021) stressed the importance for organisations to assess and enhance their cybersecurity measures to combat the emerging threats brought about by the pandemic.

1.2 Problem statement

Due to the pandemic causing a rapid shift to digitalisation, concerns regarding cybersecurity had emerged (Pandey & Pal, 2020). Table 1.1 provides a summary of reported cyberattacks across various countries, illustrating the extent of these threats and their correlation with remote work activities.

Table 1.1: Top 2 Countries from Each Continent During the COVID-19 Pandemic based on the Global Cybersecurity Exposure Index

Continent	Top 2 Least Scores	Top 2 Worst Scores
Europe	1. Finland (0.110)	1. Bulgaria (0.483)
	2. Denmark (0.117)	2. China (0.483)
Oceania	1. Australia (0.131)	1. Papua New Guinea (0.755)
	2. New Zealand (0.179)	2. Solomon Islands (0.762)
Asia	1. Japan (0.138)	1. Myanmar (0.910)
	2. South Korea (0.269)	2. Afghanistan (1.000)
North America	1. United States (0.145)	1. Mexico (0.483)
	2. Canada (0.207)	2. Nicaragua (0.600)
Africa	1. Mauritius (0.200)	1. Nigeria (0.614)
	2. South Africa (0.417)	2. Tunisia (0.614)
South America	1. Chile (0.469)	1. Bolivia (0.783)
	2. Argentina (0.514)	2. Venezuela (0.807)

Source: PasswordManagers (2020)

The Cybersecurity Exposure Index (CEI) is a comprehensive metric that evaluates the level of exposure to cybercrime across different countries, with scores ranging from 0 to 1. A higher score indicates greater vulnerability and exposure to cyber threats, highlighting the relative state of cybersecurity within a specific nation. This index is vital for understanding the global landscape of cybersecurity, guiding policymakers, businesses, and organisations in making informed decisions regarding cyber defences and resource allocation.

In the context of this research, South Africa stood out as a critical case study. Although it ranked second in Africa for the least exposure to cybercrime, with a score of 0.417, placing it 34th out of 85 countries overall, this position is still concerning. When compared to countries like Mauritius, which had a significantly lower score of 0.200, South Africa's relatively high exposure indicates underlying vulnerabilities. Given the economic and technological landscape of South Africa, understanding its cybersecurity challenges is crucial, especially as the nation increasingly integrates digital solutions across various sectors.

The effects of COVID-19 on South African-based organisations have proven to be significant and necessitated urgent attention. During the pandemic, many South African businesses, like those around the world, shifted to remote working models, which heightened the risk of cyber threats. Despite South Africa's position as one of the least exposed countries in Africa, its overall score indicated a noteworthy susceptibility when analysed alongside other nations. For instance, while Australia and New Zealand maintained low scores of 0.131 and 0.179, respectively, South Africa's score placed it in a vulnerable position - the risks were amplified due to inadequate cybersecurity infrastructure and increased online activity during lockdowns. Hence, investigating how organisations in South Africa adapted to these challenges, and the

implications for their cybersecurity resilience, was vital in understanding the broader impacts of the pandemic.

Several research gaps were identified at the intersection of cybersecurity and COVID-19 (Hernández, 2023). The areas of research that needed to be addressed included: the rise in cybersecurity threats during the pandemic (Yadav, 2021); the impact on the cybersecurity workforce, and the use of technology in the fight against COVID-19 (Baz et al., 2021); the effects of digitalisation (Pandey & Pal, 2020); and the evolution of cybersecurity threats, especially social engineering, and how it had been linked to the spread of COVID-19 (Hijji & Alam, 2021).

Due to the rapid digitalisation, cybercriminals had more opportunities to take advantage of weaknesses in the organisations' information systems (Saeed et al., 2023a). This meant that the intensity of cybersecurity-threats increased, as the proportion of time spent online increased (Ashraf et al., 2022). Thus, it was important to conduct a study to determine how COVID-19 had attributed to that increase (Chigada & Madzinga, 2021).

Conducting research on cybersecurity resilience in South Africa (SA) is especially important due to the country's unique socioeconomic, geopolitical, and technological environment (Bote, 2019). Understanding the SA cybersecurity landscape requires considering factors such as the country's history of political instability, economic inequality, and digital divide (Mphatheni & Maluleke, 2022). This holds true for this study analysing the effects of COVID-19 on cybersecurity in SA organisations, because the pandemic brought about unprecedented changes to the socioeconomic landscape in the country. With the sudden shift to remote work and digital operations, many organisations had to quickly adapt their cybersecurity measures to the changing landscape. SA's geopolitical environment also played a role in these organisations' ability to maintain cybersecurity resilience during the pandemic (Calandro, 2020). The country has faced challenges in the past with high levels of cybercrime due to factors such as limited law enforcement resources and a lack of cybersecurity awareness amongst the general population (Shingange, 2022). This study analysing the effects of COVID-19 on cybersecurity in SA organisations was crucial in understanding the effects of the pandemic on their cybersecurity posture.

1.3 Research questions and objectives

The rising reliance on digital technology and the lack of adequate defences made SA organisations bigger targets for cybercriminals. A thorough investigation into the problem was

required because of COVID-19, to gauge its effects on the cybersecurity of SA organisations. The answers to the "how" portion of the questions was offered by Engeström's Activity Theory Framework (ATF), which was used in this study. The researcher conducted a qualitative study to respond to the following research questions:

Primary Research Question: What are the COVID-19 effects on cybersecurity in organisations in SA?

- Secondary Research Question 1: How has COVID-19-induced remote work threatened cybersecurity in organisations based in SA?
- Secondary Research Question 2: How has COVID-19 changed the way organisations practise cybersecurity awareness in SA?
- Secondary Research Question 3: By being based in SA, how have organisations become more appealing to COVID-19 cybersecurity-threats?
- Main research objective: The research objective was to investigate the effects of COVID-19 on cybersecurity practices in SA organisations, with the aim of identifying potential vulnerabilities and devising efficient tactics to enhance cybersecurity and address the challenges arising from the pandemic. This objective specifically focused on analysing the "cybersecurity management activity" within the broader organisational context, which involved implementing processes and systems to protect digital assets from cyber-threats.

1.4 Intended contributions

The intended contribution of this research study was to provide insight into the specific effects of COVID-19 on cybersecurity in SA organisations. This included: the impact of COVID-19 and remote work on cybersecurity; the emergence and development of cybersecurity-threats during the pandemic; and the importance of improved cyber-awareness practices in managing risks during COVID-19. By using Engeström's ATF and conducting a qualitative study, the researcher aimed to answer the research questions and provide practical recommendations for enhancing cybersecurity in SA organisations, both during and after a crisis. The study's findings and recommendations are expected to have a significant impact on further research and the cybersecurity landscape in SA.

1.5 Chapter 1 Summary

Chapter 1 establishes the research context by discussing the effects of the COVID-19 pandemic on business operations and cybersecurity. It outlines the significant challenges organisations

encountered while adopting digital technologies during the pandemic, which subsequently led to an increase in cybersecurity threats. The chapter identifies critical research gaps at the intersection of cybersecurity and COVID-19, with a particular focus on the South African landscape. It also articulates specific research questions intended to explore the effects of the pandemic on cybersecurity practices within organisations. Additionally, the chapter highlights the intended contributions of the study, which aim to enhance understanding of these dynamics and improve cybersecurity resilience amongst South African organisations.

Chapter 2: Literature review

This chapter defines cybersecurity and cybercrime. It also provides an analysis of the current state of the cybersecurity landscape in SA and a description of COVID-19. The chapter investigates the cybersecurity-threats posed by cybercrime to organisations. Academic theories and their relevance in the study are discussed. The researcher elucidates the ATF, emphasising its fundamental concepts and its implementation in real-life scenarios within the cybersecurity realm. Finally, the researcher explores the framework's relationship with information systems, followed by an examination of whether its underlying rationale is applicable for this type of research.

2.1. Cybersecurity defined

Academic discussions about "cybersecurity" in the past have been vague and influenced by personal opinions, rather than by an objective analysis. As a result, three scholars conducted a study to develop a comprehensive and standardised definition. Based on their research, they crafted a unique and meticulous definition, that applied to the specific realm of cybersecurity examined in this study. Their definition was presented as:

> *"Cybersecurity is the organization and collection of resources, processes, and structures, used to protect cyberspace and cyberspace-enabled systems, from occurrences, that misalign de jure from de facto property rights"* (Craigen et al., 2014:17).

Comprehensive cybersecurity measures involve more than just traditional perimeter defences, such as firewalls and antivirus solutions (Thomas & Sule, 2023). Proper cybersecurity management necessitates skilled personnel, well-established threat identification and response protocols, and unyielding systems capable of withstanding potential attacks (Furnell, 2021). To ensure a competent cybersecurity strategy, collaboration with external stakeholders such as suppliers, customers, and industry partners, along with internal departments including information technology (IT), risk management, legal and compliance is critical (Colicchia et al., 2019). Continuous learning and adaptation of best practices, trends, and threats in the cybersecurity field is essential. However, the above conceptualisation of cybersecurity poses a challenge, as it does not offer definitive structures, procedures or resources, as individual organisations may interpret cybersecurity requirements differently based on their unique needs and available resources.

Cybersecurity measures cannot be universally applied and should be flexible to adapt to varying circumstances, based on factors like size, industry, and risk profile (Sungkur & Maharaj, 2021). This implies that organisations must customise their security plans to suit their specific requirements without being overly rigid. It is crucial to define cybersecurity in a non-prescriptive manner (Barry et al., 2022). This highlights the fact that cybersecurity is continuously evolving; thus, it is essential to avoid fixed definitions.

It is important to protect cyberspace and associated systems by utilising defence tools and techniques, such as intrusion detection and prevention systems, firewalls, encryption, and antivirus software (Zheng et al., 2022). This inclusive protection strategy is aimed at addressing both intentional and unintentional threats resulting from system vulnerabilities or user errors, as well as natural disasters or power outages. This phrase underpins the vital nature of cybersecurity in the present interconnected world, where cyberspace plays an essential role in almost every aspect of human life (Goutam, 2021). Therefore, the implementation of effective cybersecurity measures is crucial to safeguard various entities, including individuals, organisations, and governments. Thus, the security of such entities relies heavily on successful cybersecurity implementation.

Lastly, the phrase “misalign de jure from de facto property rights” pertains to distinct aspects of ownership and control, which have been extensively studied in relation to cybersecurity and digital assets. Digital assets refers to digital representations of value (Popescu, 2021). Examples of digital assets include cryptocurrencies such as bitcoin, Ethereum, and Litecoin, which are increasingly being used in industries such as banking, real estate, and healthcare (Rejeb et al., 2021). The phrase forms a part of Ostrom and Hess’s (2011) property rights framework, which includes seven elements: access, extraction, contribution, removal, management, exclusion, and alienation. Craigen et al. (2014) define cybersecurity incidents as actions or events that create a discrepancy between actual (de facto) and perceived (de jure) property rights, whether intentionally or unintentionally, and whether detected or unknown. This suggests that cybersecurity measures may differ from legal protections on paper and implementing both standards is critical to securing cyberspace and its related systems (Al-Hawamleh et al., 2020).

2.1.1 How cybersecurity is threatened

The demand for cybersecurity has noticeably increased in recent years due to the rise in both the prevalence and complexity of cyber-threats (Grobler et al., 2021). Cybercrime has emerged as a major global issue, posing significant challenges for cybersecurity (Khiralla, 2020). The

effects of cybercrime are extensive, with individuals, organisations, and governments experiencing severe negative consequences.

2.2 Cybercrime defined

The increasing use of the Internet has led to a rise in cybercrime, which is a growing concern in modern society (Arab, 2020). While researchers have various definitions of cybercrime, many associate it with digital technology or the Internet. However, cybercrime's multifaceted nature makes it difficult to define comprehensively. As a result, countries can categorise cybercrime based on their unique perspectives to better understand its impact and characteristics (Bhowmik, 2023).

Protrka (2021) proposed that the United Kingdom (UK)'s Crown Prosecution Service classify cybercrime into two categories: cyber-dependent and cyber-enabled crimes. This categorisation assists law enforcement officials in comprehending and handling different types of cybercrime effectively.

Cyber-dependent crimes are solely reliant on IT and include activities like hacking (Maimon & Louderback, 2019). These crimes are committed through the use of a computer system or electronic communication tools, such as the Internet or mobile devices (Brosnan, 2021). Illegal acts include hacking, phishing, and identity theft. The prevalence of cyber-dependent crimes is growing globally, and criminals are becoming more sophisticated in their methods (Chowdhury & Fahim, 2020). To combat these crimes, education, awareness and robust cybersecurity measures are necessary (Bada & Nurse, 2019).

Cyber-enabled crimes require the integration of technology into traditional crimes, such as online fraud or cyberbullying (Nwankwo et al., 2022). These crimes involve the use of computer technology or the Internet (Akdemir & Lawless, 2020). Various criminal acts make use of these methods, including cyberstalking, identity theft, hacking, and malware attacks (Al-Khater et al., 2020). As technology becomes more sophisticated, cyber-enabled crimes have become more complex, making it challenging for law enforcement and cybersecurity professionals to prevent and detect them (Maimon & Louderback, 2019). Addressing cyber-enabled crimes requires collaboration amongst diverse stakeholders, such as law enforcement agencies, companies, and academic institutions (Dupont & Whelan, 2021).

2.2.1 Types of cybercrime

Exploring why people partake in cybercrime and its consequent effects on individuals and establishments, may benefit from the adoption of criminological, sociological, and

psychological theories. Social Identity Theory (SIT), for example, offers one probable approach to understanding the motivation behind cybercrime. According to SIT, individuals may undertake criminal activities as a means of attaining social status or membership in a specific group (Tajfel & Turner, 2004). Such groups could comprise hackers or online communities that encourage illegal actions. Psychological Strain Theory (ST) presents a valuable framework that suggests that people may resort to criminal behaviour as a coping strategy against stressors and negative emotions that plague their lives (Agnew & White, 1992). ST expounds on the reasons why individuals who feel marginalised or powerless in their daily lives, resort to online crime to exert control over their environment or gain a sense of agency.

According to Shaw and McKay's (1942) Social Disorganisation Theory (SDT), the aspects of a community can heavily impact the incidence of delinquency. Communities that have high poverty rates, high levels of unemployment, and frequent residential mobility, are more susceptible to social disorganisation. This, in turn, can lead to elevated criminal activity such as cybercrime (Shaw & McKay, 1942). It suggests that individuals who came from disadvantaged backgrounds are more inclined to participate in online criminal activities for the purpose of financial gain. The implications of cybercrime for organisations can be elucidated by employing an organisational theory, such as Social Exchange Theory (SET), which focuses on the impact of interpersonal and organisational relationships on attitudes and behaviours (Blau, 1964). It argues that individuals may disengage or resort to dysfunctional behaviours if negative consequences result from the involvement in cybercrime. Consequently, organisations that are repeatedly targeted with cyber-attacks are at risk of losing the trust and support of their staff, which can have disastrous repercussions. Figure 2.1 illustrates an array of categories showing various subtypes of cybercrime that are often interconnected during a cyber-attack. Given the increasing role of technology in society, the threat of cybercrime is ongoing, making it imperative to identify distinct types of cybercrime explained by relevant theories.

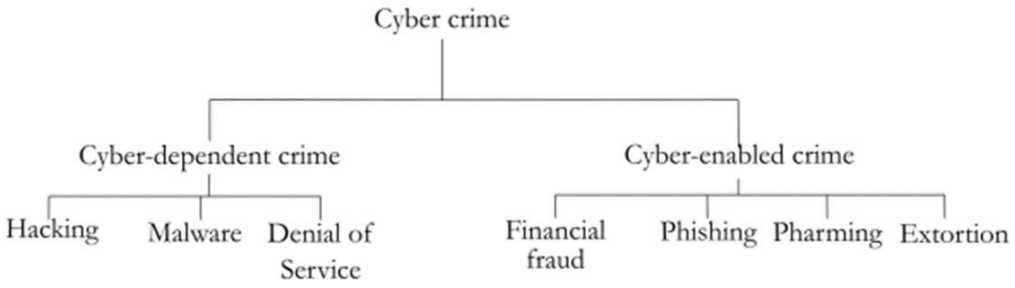

Figure 2.1: Types of Cybercrime

Source: Lallie et al. (2021)

2.2.1.1 Hacking

Hacking is an illegal activity where an individual gains unauthorised access to a computer system or network to obtain sensitive information or disrupt its normal operations for personal, political, or financial reasons (Steinmetz, 2022). The reasons behind hacking can be attributed to ST, which suggests that individuals engage in illegal activities, including hacking, when they encounter obstacles or lack legitimate opportunities to achieve their goals (Agnew & White, 1992). The Social Learning Theory (SLT) also influences hacking, as people may be influenced by their peers to engage in such activities (Bernatzky et al., 2021). ST provides insights into hacking behaviours, explaining that individuals engage in such activities when they experience stressful life events, such as financial hardship or social exclusion, that limit their opportunities to achieve their goals. Research studies have supported this connection between ST and hacking, finding strain and stressful life events to be significant predictors of hacking amongst college students (Hay & Ray, 2020). The studies identified that cybercrime involvement, including hacking, was significantly predicted by strain, social learning, and low self-control (Stalans & Donner, 2018). While ST provides a useful framework for understanding hacking behaviours, not all individuals experiencing stressful life events will engage in hacking. Other factors, such as personality traits and social factors, may also influence such behaviours (Choi et al., 2019). Prevention strategies for hacking should consider individual, social, and environmental factors to adopt a multidimensional approach.

2.2.1.2 Malware

Malware is a type of software designed to harm or disrupt computer systems without user consent (Ngo et al., 2020). Examples of malware include viruses, trojans, and spyware (Prasad & Rohokale, 2020). Rational Choice Theory (RCT) can help determine the motives behind malware creation and distribution. In RCT, individuals engage in cybercrime when they believe that the rewards outweigh the potential negative consequences (Cornish & Clarke, 1989). Financial gain, political motivations, or a desire for retaliation may drive malware creators. Studies on the link between RCT and malware indicate that individuals engage in cybercrime for goals such as financial gain, status, or excitement (Collier et al., 2020). People's incentives to create malware are influenced by their perception of benefits and the likelihood of being detected (Morrison, 2022). RCT provides valuable insights into understanding how cybercriminals make decisions, which can help organisations protect themselves from potential attacks.

2.2.1.3 Denial-of-service attack

Denial-of-service (DoS) attacks involve deliberately overwhelming a website or network with excessive traffic or requests to disrupt its operation, making it challenging for authorised users to access it (Gulihar & Gupta, 2020). According to SDT, the absence of supervision, regulation, and social control in cyberspace could lead to a breakdown of legal norms and collective efficacy, creating an environment conducive to cybercrime (Shaw & McKay, 1942). In SDT, the absence of supervision, regulation, and social control in cyberspace can lead to the breakdown of legal norms and collective efficacy, creating an environment that encourages cybercrime. DoS attacks may be launched by hackers to gain recognition or express dissatisfaction with certain institutions or belief systems. These motivations align with SLT, which posits that individuals learn through observing and imitating the actions of others (Bandura & Walters, 1977). Consequently, hackers may engage in DoS attacks for their perceived self-interests.

2.2.1.4 Financial fraud

Financial fraud is a form of cybercrime that involves using manipulation or deception techniques to deceive individuals or organisations into giving away valuable assets or money (Reurink, 2019). Fraud Theory (FT) offers insight into fraudulent activities by explaining the thought processes behind them. The fraud triangle model, a key aspect of FT, emphasises the significance of pressure, rationalisation, and opportunity. These elements can lead to financial fraud through a calculated analysis of benefits, abilities, and prospects. To gain a deeper understanding of financial fraud, researchers have explored the connection between FT and various studies. Individuals with access to organisational resources were more likely to commit fraud than those who did not (Hashim et al., 2020). People who justified their actions were more inclined to engage in financial fraud (Utami et al., 2019.

2.2.1.5 Phishing

Phishing is classified as a deceitful and fraudulent technique that involves sending fake emails or setting up misleading websites to trick people into providing their sensitive information, such as bank account details, passwords, or social security numbers (Orunsolu et al., 2022). SET underpins the fundamentals of such cybercrime, where attackers rely on tactics such as persuasion and psychological manipulation to manipulate victims into revealing their information (Musuva, 2019). To increase the perpetrators' chances of success, phishing attacks exploit cognitive biases such as urgency, authority, and trust. The success of phishing attacks

relies heavily on SET, as it involves deceiving victims by posing as trustworthy entities or using other means of manipulation. Research has established that attackers can control the thought process of their targets through psychological manipulation and persuasion techniques, which increases their likelihood of success (Wang et al., 2021). These attacks employ cognitive biases to increase their effectiveness, making it crucial to educate individuals and organisations on how to mitigate such risks (Shahbaznezhad et al., 2021). For example, attackers may use logos and brand names of reputable companies or false testimonials to lure victims into providing their sensitive information (Alabdan, 2020).

2.2.1.6 Pharming

Pharming is a type of cyber-attack that involves manipulating a website's domain name system (DNS) records to redirect users to a fraudulent website (Alkhalil et al., 2021). This fake website appears identical to the genuine one and prompts users to provide sensitive personal information, such as usernames and passwords, which can be exploited by the attacker. Pharming attacks can be seen as an example of a crime facilitated by modern technology, requiring a certain level of technical expertise to execute (Kalajžić, 2019). The success of the attack depends on the vulnerability of the target website and its users, and the lack of effective guardianship, such as proper website security measures, can make it easier for attackers to carry out such attacks. Routine Activity Theory (RAT) posits that crimes increase with motivated offenders, suitable targets, and lack of guardianship. Badamasi et al. (2019) connect pharming to RAT, highlighting the role of offenders and vulnerable targets driven by financial or personal motives for successful attacks.

2.2.1.7 Extortion

Extortion is the illegal practice of obtaining goods, services, or money through coercion or threats (Abdulhameed, 2021) with significant impacts on individuals and society. Deterrence Theory (DT) explains the relationship between extortion and crime deterrence (Stigler & Becker, 1977). Their study revealed that increasing the costs of punishment, like raising fines or imprisonment severity, can deter potential extortionists. The threat of detection and arrest acts as a significant deterrent against extortion (Shavell, 1992). Deterrence can also prevent organised crime, such as extortion rings that use threats, violence, or blackmail to coerce money or resources from individuals or businesses (Ryan, 2020). Enhancing the likelihood of arrest and conviction for these groups can effectively deter their activities (Paternoster, 2019).

2.3. COVID-19 defined

The pandemic caused by COVID-19 rapidly escalated into a worldwide crisis, because of the virus's highly contagious nature. To mitigate the spread of the virus, numerous countries implemented rigorous lockdowns and physical distancing policies. These measures were implemented with the aim of reducing the rapid transmission of the virus and inhibiting its further spread. For this study, COVID-19 is defined as:

> *"An infectious disease primarily transmitted through droplets of saliva or nose discharge, when the infected individual sneezes or coughs"* (Xu et al., 2020:1).

The COVID-19 pandemic has heightened concerns about cybersecurity-threats, leading researchers to examine theories like the Theory of Planned Behaviour (TPB). With TPB, individuals are driven by their intentions, influenced by their attitude, social norms, and perceived control over their actions (Ulker-Demirel & Ciftci, 2020). In this pandemic era, the TPB sheds light on why people might be more vulnerable to cyber-attacks. Individuals with a positive or neutral view towards risky online behaviours may be more prone to engaging in them due to increased online activity during the pandemic, potentially aggravating feelings of social isolation (Ulker-Demirel & Ciftci, 2020).

2.3.1 SA organisations during COVID-19

Apakah (2021) highlights the importance of analysing the effects of COVID-19 on cybersecurity in organisations situated in African countries such as SA. This importance stemmed from the following reasons. Firstly, SA, with its burgeoning economy and a significant online presence, is highly susceptible to cyber-attacks, which had become more intense due to COVID-19 (Ndemo, 2021). Hence, comprehending how COVID-19 has affected cybersecurity was crucial in mitigating risks and bolstering resilience against cyber-attacks. Secondly, the pandemic has adversely affected numerous sectors of the SA economy, such as tourism, hospitality, and events, resulting in income and job losses (Sucheran, 2022). Since organisations in these sectors depend heavily on digital operations, understanding how the pandemic may have intensified these cybersecurity risks is vital. Thirdly, social-economic inequity in SA has made it increasingly challenging to defend against cyber-attacks, as the digital divide and lack of cybersecurity knowledge in some communities has heightened vulnerability to such attacks (African Union, 2020). Consequently, examining the effects of COVID-19 on cybersecurity practices will provide organisations with valuable insights into how the pandemic has impacted the cybersecurity-threats, mitigation strategies, and policies.

Thus, such a study is critical in aiding decision-making processes, building organisations' resilience to cyber-attacks, and ensuring business continuity, even during crises.

Organisational analysis is crucial for comprehending the challenges and opportunities they encounter, as well as the attitudes of their employees towards them. Organisation size varies significantly based on industry, purpose, and management structure, ranging from a small group of individuals to several thousand or even millions (Longo, 2023). Small-sized organisations exhibit greater agility and adaptability, while larger ones have more resources, providing an advantage in their respective industries (Houston, 2019). The optimal size of an organisation is determined by its goals and available resources, as per Cabanias (2019). Research within an organisation is crucial for identifying critical performance and competitiveness-enhancing factors (Ubaid, 2023).

Identifying skills gaps and training requirements can be achieved through specific training programmes (Di Sabato & Savov, 2023). Organisations possess a unique culture and structure that can considerably shape employee performance and behaviour, distinguishing them from companies or firms. Research suggests that cultural factors play a crucial role in creating a satisfying and stable work environment, thereby retaining employees (Cherian et al., 2021). Organisational research offers crucial insights into the functioning of departments, teams, and individuals, enabling more informed decision-making regarding human resources.

2.4 ATF defined

The ATF provides a comprehensive framework for understanding the various elements and relationships within an activity system. The ATF builds on Leontiev's (1978) work, identifying six key elements: subject, tools, community, division of labour, rules, object, resulting in the outcome (Figure 2.2), which aid in comprehending the intricate interrelationships amongst various elements in activity systems, particularly in organisational contexts (Roberts, 2020).

2.4.1 The activity

Activities are systematic arrangements of human actions and experiences that occur within a specific socio-historical context (Engeström, 1987). Activities are specific actions performed by humans in a cultural and societal environment, influenced by interactions between individuals and their environment, resulting in a dynamic and evolving process, and providing insight into the evolving nature of human action in specific contexts (Nardi, 1996).

2.4.2 The elements

The Subject element refers to the individuals or groups actively engaged in the tasks and working towards achieving the object. These subjects are the participants involved in the activity and play a central role in the system (Engeström, 2001).

The Tools element, an important element in the framework, encompasses the resources, technologies, and materials utilised to support and facilitate the activity. They range from physical tools to digital platforms and knowledge resources. These tools play a crucial role in enabling individuals or groups to accomplish the objectives of the activity system (Engeström, 1987).

The Community element recognises the significance of social interaction and collaboration within activity systems. It involves the formation of a community that facilitates knowledge sharing, support, and coordination amongst the individuals or groups involved. The community provides an environment for collective learning and problem-solving (Engeström, 2001).

The Division of Labour element refers to the allocation of tasks and responsibilities amongst individuals or groups within the activity system. It recognises that different roles and expertise are necessary to achieve the objectives of the activity. This ensures efficient utilisation of resources and promotes specialisation in the system (Engeström, 2001).

The Rules element acts as the guidelines, regulations, and procedures that govern the activity system. They provide structure, norms, and standards that dictate how the activity should be conducted. Compliance with these rules is vital for effective functioning and coordination within the system (Engeström, 2001).

The Object element is the action that is performed to achieve the outcome, and the outcome is the transformative result of the subject's active engagement with an activity (Hasan & Banna, 2012).

The Outcome of the activity is influenced by the complex interplay of the ATF elements, with the object element and its underlying actions serving as a key driving force in shaping the outcome (Engeström, 2001). As shown in Figure 2.2, the outcome of the ATF is not considered as a separate element but rather as the result or consequence of the activity system (Engeström, 1987).

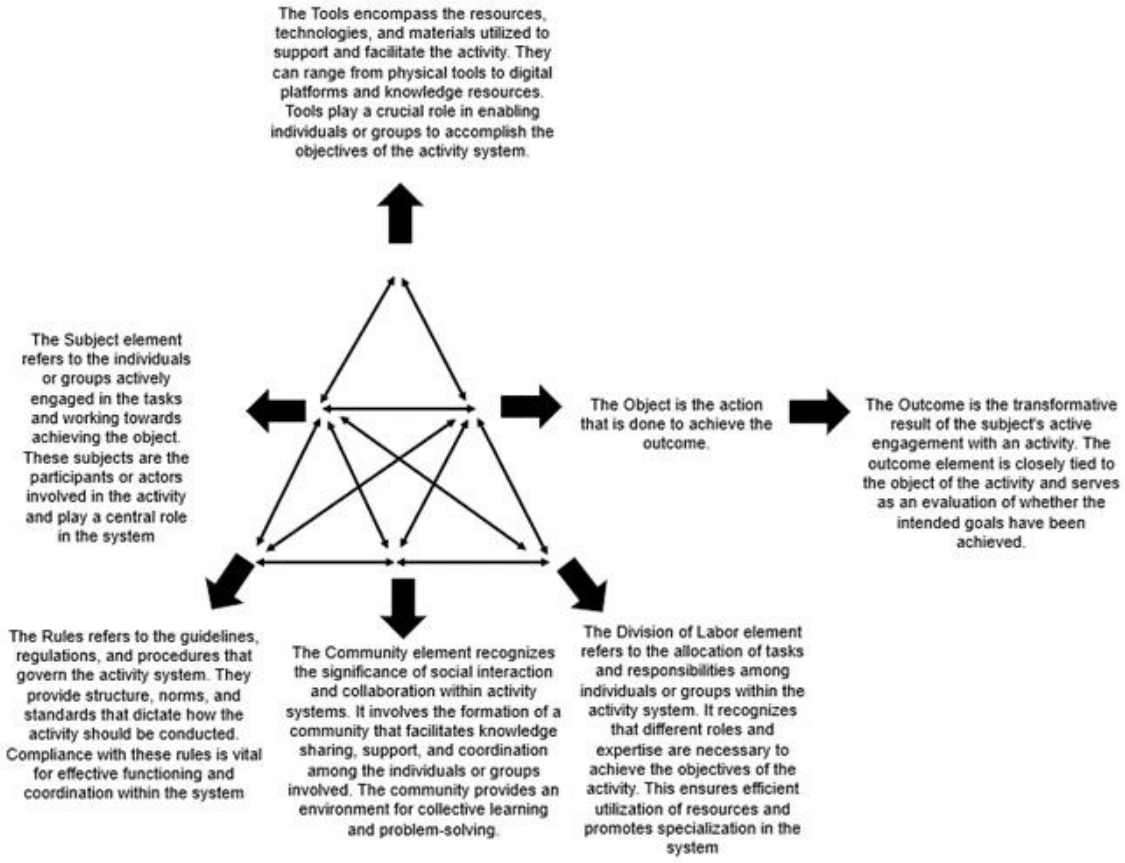

Figure 2.2: Activity Framework Diagram.

Source: Engeström (1987)

2.4.3 ATF appropriateness for the current study

The utilisation of frameworks, including the Social-Technical Systems (STS) framework and the Unified Theory of Acceptance and Use of Technology (UTAUT), has been customary to analyse cybersecurity in different contexts. The research context revealed that neither of these frameworks is entirely suitable for this study. The inadequacy is primarily due to their inability to address the unique systemic and contextual factors, as well as the specific challenges posed by the pandemic.

Firstly, the STS framework explores the interplay between social and technical aspects within a system (Cherns, 1976). The system's effectiveness is influenced by comprehending not only its technical aspects but also the social context in which it operates. This framework may not be fully applicable for studying the impact of COVID-19 on cybersecurity in SA organisations. While the STS framework focuses on the interplay between social and technical aspects, it may overlook the significance of user input and the impact on system usability (Orlikowski, 2000),

which may limit the ability to capture the nuances of real-world work environments. The lack of explicit guidance or methods for understanding dynamic interactions between technical systems and social context (Geels, 2004), further hinders its suitability for studying the effects of COVID-19 on cybersecurity.

The ATF is more applicable, as it explicitly emphasises the social and organisational dimensions. User involvement in system design and development is important and is crucial in understanding the effects of COVID-19 on cybersecurity (Nardi, 1996). The need to understand work practices and their influence on system design and usability, aligns well with studying the impact of COVID-19 on cybersecurity (Kaptelinin & Nardi, 2006). The authors provide tools like activity diagrams for analysing and designing socio-technical systems, offering a comprehensive understanding of the dynamics impacted by COVID-19. The ATF approach is more suitable for studying the impact of COVID-19 on cybersecurity in SA organisations.

The UTAUT primarily focuses on individual-level behaviours and attitudes towards technology adoption and use (Venkatesh et al., 2003). While it considers contradictions and tensions (Orlikowski, 2000), it does not extensively address the organisational factors and dynamics influencing technology acceptance, adoption, and use (Agarwal & Prasad, 1998). UTAUT does not provide specific guidance for designing interventions to address the complex socio-technical challenges (Leonardi, 2012). The ATF emphasises collective action, social collaboration, and the broader social and organisational contexts of technology adoption and use (Engeström, 1987). It recognises the presence of contradictions and tensions within social systems and provides a framework to analyse and address them (Nardi, 1996:7-16). The ATF offers a comprehensive framework for studying the broader impacts, transformations, and consequences of technology implementation within a social context (Karanasios, 2018). It also provides practical tools for intervention and change management within socio-technical systems (Pahl-Wostl, 2007). The ATF was found to be more suitable for studying and analysing the impact of COVID-19 on cybersecurity. It offered a holistic perspective that accounts for the social, collaborative, and organisational aspects involved in technology adoption and use. The framework provides a method to comprehend contradictions, explore broader contexts, and devise strategies to tackle intricate socio-technical issues.

The ATF was suitable for this study because it focused on understanding and resolving problems within a specific activity, which in this case was the cybersecurity management activity during the pandemic (Kshetri, 2021). The cybersecurity management activity

encompasses various processes, practices, and systems implemented by organisations to protect their digital assets from cyber-threats; it refers to the strategic planning, implementation, and oversight of initiatives that aim to protect and manage an organisation's digital assets and infrastructure (Limba et al., 2017). This includes activities like risk assessment, development of cybersecurity policies and procedures, incident response planning, employee training and awareness programmes, regular monitoring and analysis of cyber-threats, and continuous improvement of security measures (Parsola, 2022). This ensures an organisation's IT systems' confidentiality, integrity, and availability, while mitigating risks and responding effectively to cybersecurity incidents (Ghelani, 2022).

The ATF enabled the researcher to analyse the interaction of cybersecurity management elements and their impact on external factors like the pandemic. The framework offers a comprehensive analysis of system dynamics, identifying potential barriers, tensions, and contradictions that could either hinder or enhance cybersecurity efforts. Within the specific activity of cybersecurity management during the pandemic, the ATF facilitated an analysis of the problems that had emerged due to the pandemic. The researcher utilised this framework to analyse the challenges and obstacles faced by organisations and individuals in managing cybersecurity in these crises. The study offers a comprehensive understanding of the complexities of cybersecurity management activity systems and their impact during the pandemic.

2.4.4 ATF appropriateness

The application of ATF in the cybersecurity research in SA, has proven to be highly appropriate. The ATF considers not only the technological aspects but also the social and cultural contexts, making it a suitable framework for examining the complexities of cybersecurity (Durst et al., 2020). Its relevance in SA is heightened because of the country's diverse population and cultural landscape. The ATF aids researchers in comprehending the processes of protecting digital assets from cyberattacks, considering social and cultural factors influencing cybersecurity practices. The increasing cybersecurity concerns in SA, as highlighted by Kritzinger et al. (2023), bolster the relevance of the ATF in this research area. It allows researchers to identify the elements involved in cybersecurity and examine their respective actions, providing a valuable tool for comprehending the factors that influence cybersecurity actions of individuals, groups, organisations, and governmental entities within the SA context. By considering the broader sociocultural context and the interdependencies amongst different

actors, the ATF provides a nuanced understanding of the cybersecurity landscape in SA (Zomer et al., 2021).

2.4.5 Past ATF applications in cybersecurity

In recent times, digital technology has witnessed a surge in the significance of cybersecurity as a critical concern. The ATF is amongst the various frameworks used by scholars in SA to navigate through the complexities of cybersecurity, such as education, training, and organisational responses to incidents. The first application focused on the transformative development of students' cyber defence consciousness over time (Kam & Shang, 2019). Through interviews and analysis of transcripts, Kam and Shang highlighted the internalisation of skills and knowledge, reliance on community support, and the division of labour in teamwork.

Karjalainen and Ojala (2023) examined the requirements for optimal in-service training in dealing with cybersecurity incidents. They identified three fundamental components and four elements of optimal training, aligning with the principles of ATF. The approach emphasises the significance of comprehensive cyber-practice in enhancing readiness and competence in real-life incidents, highlighting the intricate interactions between individuals, tools, and contexts. Østby and Kowalski (2022) focused on crisis management exercises to facilitate learning and organisational change. By implementing a triple-loop learning process and utilising reflection and debrief techniques, they found that these exercises supported learning and contributed to organisational change in the field of information security management.

2.4.6 ATF contradictions explained

Kuutti (1996) defines contradictions as disparities in an activity system due to norm conflicts, communication issues, and resource shortages. Engeström (1987) introduced the four stages of contradiction model, which addresses conflicts and contradictions through cooperative learning and advancement as potential resolutions. He proposed that primary contradictions in cybersecurity can be categorised into subject-object, subject-tool, object-outcome, community-tool, and community-division of labour.

Secondary contradictions arise when two or three fundamental elements conflict, like the labour-outcome conflict in IT professionals' ability to fulfil their duties, leading to cybersecurity issues (Kuutti, 1996). Tertiary contradictions, consisting of three or four critical elements, can pose significant cybersecurity-threats. For instance, the subject-community-division of labour-outcome contradiction may occur due to the lack of IT professional support,

leading to cybersecurity failures (Kuutti, 1996). Lastly, there are four contradictions that affect all six critical elements simultaneously, potentially leading to systemic issues. An illustration of the subject-object-division of labour-outcome conflict may arise when IT experts are ill-equipped to handle emerging threats, resulting in unfavourable outcomes for system security (Kuutti, 1996).

2.4.7 ATF and its relationship with information systems

The utilisation of information systems within organisations is inherently linked to individual employee behaviour, subsequently affecting how such systems are conceived, implemented, and designed (Mursu et al., 2007). The ATF has enabled scholars to understand how information systems within organisations shape human behaviour, aiming to enhance human activities and optimise corporate objectives (Iyamu & Shaanika, 2019). To explore the interplay between human, social, and technological systems, the application of the ATF supports the creation and development of information systems by assessing various system elements and their complementary activities within the operational environment (Iyamu & Shaanika, 2019).

2.5 Chapter 2 Summary

Chapter 2 offers a thorough exploration of cybersecurity and cybercrime, defining essential concepts while analysing the current cybersecurity environment in South Africa amid the COVID-19 pandemic. This chapter outlines the escalating threats that cybercrime poses to organisations and discusses pertinent academic theories that elucidate the motivations behind cybercriminal behaviour. The Activity Theory Framework (ATF) is introduced, showcasing its structure and usefulness in understanding the intricate challenges of cybersecurity management within organisational settings. It stresses the dynamic nature of cybersecurity and the necessity for customised strategies to tackle specific organisational issues, especially given the intensified risks during the pandemic. Finally, the relevance of the ATF is underscored due to its capability to navigate the interaction between technical and social aspects of cybersecurity practices.

Chapter 3: Research methodology

The selection of a research approach is a crucial stage in any research endeavour, and this study justified its choice by providing a rationale for the methodology used (Saunders et al., 2009). Before commencing the research process, it is crucial to define the study's objectives and methodology. The research onion model, introduced by Saunders et al. (2009), visually represents the research phases (Figure 3.1).

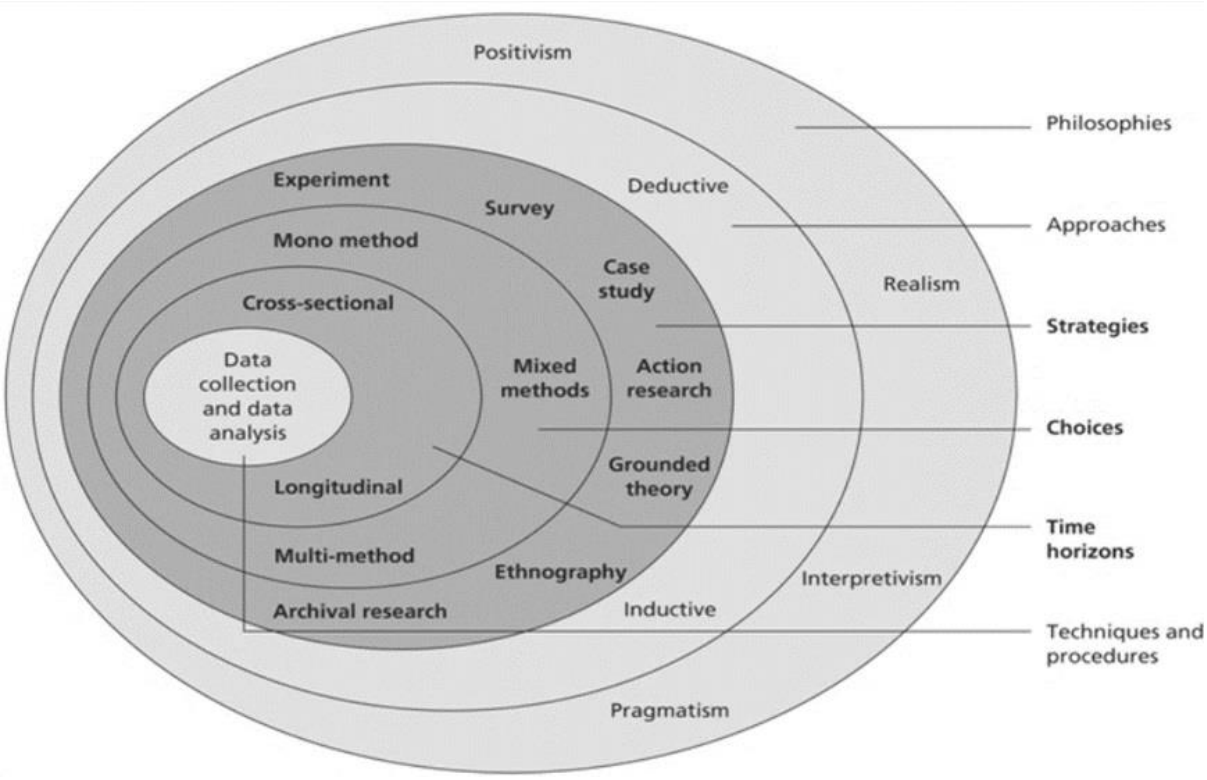

Figure 3.1: The Research Onion.

Source: Saunders et al. (2009)

3.1. Research philosophy

The adoption of a research paradigm or philosophy results in two primary benefits (Saunders et al., 2009). Research approaches, including pragmatism, positivism, realism, and interpretivism, guide and select effective techniques in various research philosophies (Mbanaso et al., 2023). Pragmatism focuses on research questions, while positivism advocates for empirical observation and quantitative analysis as the only acceptable methods for enhancing scientific knowledge. The realism paradigm employs both quantitative and qualitative methods to study the social world, taking into account personal experiences and biases.

3.1.1 Epistemology and ontology

Epistemology refers to the branch of philosophy that examines how knowledge is acquired, justified, and understood (Sol & Heng, 2022). It deals with questions such as how knowledge is obtained, what constitutes valid knowledge, and how we can determine the truth or reliability of our beliefs and claims. Ontology refers to the branch of philosophy that explores the nature of existence and reality. It deals with questions related to what things exist, what their essential properties are, and how these things are related to each other (Khatri, 2020).

Interpretivism is an epistemological approach that focuses on understanding individuals' subjective experiences and interpretations of the social world (Pervin & Mokhtar, 2022). It recognises that knowledge is constructed through interpretive processes and emphasises the importance of understanding the meanings and interpretations that individuals attribute to their experiences. Interpretivism is chosen to analyse subjective cybersecurity expert experiences in SA organisations, focusing on COVID-19-related threats, aiming to understand and interpret their perspectives.

Subjective ontology is a philosophical perspective that acknowledges and recognises the existence of different subjective experiences, perceptions and realities (Bauchan. 2023). It emphasises that individuals and organisations have their own unique perspectives, values, and contexts that influence their understanding of the world. By adopting subjective ontology, the study acknowledged the variability in cybersecurity needs and practices amongst organisations and emphasises the importance of individual realities in shaping knowledge and decision-making processes. This ontology aligned with the goal of recognising and considering the diverse experiences and perspectives of cybersecurity experts in SA organisations. These philosophical concepts allowed for an inductive approach, enabling the study to collect and analyse data from cybersecurity experts' experiences and perspectives, ultimately uncovering meaningful insights and patterns.

3.1.2 Inductive and deductive

A study that adopts a subjectivism ontological paradigm and interpretivism epistemology is better suited for an inductive approach (Al-Ababneh, 2020). The researcher conducted 30 semi-structured interviews (Appendix A) to understand the subjective experiences and perspectives regarding the impact of COVID-19 on cybersecurity in SA organisations. Inductive reasoning enabled the researcher to extract insights from participant observations and experiences. By focusing on the participants' subjective viewpoints, the study aimed to capture the diverse

perspectives and nuances associated with the complex phenomenon of COVID-19's impact on cybersecurity in SA organisations.

In subjectivism and interpretivism, a deductive approach may not be the most suitable, as it typically involves testing pre-established theories or hypotheses and making predictions based on general principles (Gilgun, 2019). The study focuses on comprehending and interpreting the subjective experiences and meanings that individuals attribute to their realities. The researcher sought to develop a rich and contextualised understanding by allowing the findings to emerge organically from the data, rather than imposing pre-established hypotheses or frameworks (Johnson & Christensen, 2017). The researcher employed thematic analysis, a qualitative data analysis technique, to carefully analyse the data collected through the interviews (Braun & Clarke, 2006).

The researcher utilised a subjectivist ontology and interpretivist epistemology to identify patterns, themes, and theoretical insights related to COVID-19's impact on cybersecurity in SA organisations. The study utilised an inductive approach to apply the ATF, aiming to derive insights from participant observations and experiences. This aligned with the goals of the ATF, which sought to understand the interrelationships and social dynamics of human activities within specific contexts (Engeström, 1999).

3.2. Research purpose

Bhattacherjee (2012) categorised research purposes into three distinct groups: exploratory, descriptive, and explanatory. Despite each category having a distinct purpose, it is frequently necessary to combine them to achieve research objectives. Exploratory research aims to establish a fundamental understanding of a specific subject and generate fresh hypotheses and concepts for future research (Stebbins, 2001). Qualitative data collection methods like interviews, focus groups, and observations are often used alongside quantitative data collection. Descriptive research aims to describe and make sense of the features of a population or phenomenon (Zegeye et al., 2009). The objective of this type of research is to provide a comprehensive account of a given situation, including relevant demographics, behaviours, attitudes, and preferences. Gathering data for such research is achieved using quantitative techniques such as surveys, questionnaires, and structured observations.

Explanatory research aims to understand the mechanisms underlying observed relationships between independent variables, often involving experimental or quasi-experimental designs to examine manipulated variables' effects. Explanatory research involves hypothesis testing and

theory creation to predict and control the phenomenon under investigation. The descriptor-explanatory approach is employed to break down research questions into sub-questions, each with unique descriptors and explanations, in order to attain a comprehensive understanding of the research topic. This approach is typically used for descriptive or explanatory research purposes (Saunders et al., 2009). This study, classified as qualitative research, was subdivided into explanatory and descriptor-explanatory categories.

The research primarily aimed to examine the impact of COVID-19 on cybersecurity practices in SA organisations and offer recommendations for improving their security measures. To attain a complete understanding of the changes in cybersecurity measures spurred on by the COVID-19 pandemic in SA, the research relied on secondary research questions. The study's conceptual framework employed Engeström's ATF to provide an in-depth view of the cybersecurity landscape during the pandemic. Using descriptive and explanatory analyses, the interactions of various actors and their roles in the framework, the author was able to highlight the multifarious nature of the cybersecurity landscape during the pandemic.

3.3. Research time

Researchers commonly use longitudinal and cross-sectional research methods in the field of social science. Longitudinal research is advantageous for tracking phenomena and gathering data over time, but it can be time-consuming and expensive, while cross-sectional research collects data at a specific moment (Rindfleisch et al., 2008). It is more efficient and cost-effective, but it provides limited understanding. Researchers must consider their research question, budget, and time constraints when choosing a methodology. In this case, a cross-sectional approach was chosen for efficiency and cost-effectiveness.

3.4. Data requirements, types and sources

The researcher conducted a thorough research by considering various data forms, origins, and demands within the methodology process, which included gathering, interpreting, and examining data. The researcher carefully selected data demands, types, and origins based on the research question, concept, and sample size to ensure a high-quality research outcome. The research project's quality and significance were significantly enhanced by data collection and analysis, utilising 30 semi-structured interviews with cybersecurity professionals in SA organisations, as shown in Table 3.1.

To enhance the research findings, organisational information such as industry and size was also collected. These data were sourced from online databases, including Google Scholar, JSTOR,

EBSCO, and PubMed, as well as university libraries and archives. The study utilised various sources to integrate interview results into existing literature, focusing on the impact of COVID-19 on cybersecurity. This involved analysing the effects on security strategies and procedures, security breaches and attacks, technology investments and upgrades, as well as remote working policies and procedures. The study gathered cybersecurity professionals' perspectives on the COVID-19 crisis, offering insights into future predictions, preparedness, and suggestions for enhancements in the field.

Table 3.1: Data Requirements, Data Types and Data Sources

Data Requirements	Data Types	Data Sources
1. Demographic information of cybersecurity professionals: Education, experience, job title, etc.	Qualitative data	Responses from 30 semi-structured interviews
2. Organisational information: Industry, size, etc.	Qualitative data	Responses from 30 semi-structured interviews
3. COVID-19 Effect on cybersecurity: Effects on security strategies, provided, security breaches, attacks, technology, investments, policies, etc.	Qualitative data	Responses from 30 semi-structured interviews
4. Online Data: Such as Google Scholar, Jstor, EBSCO, PubMed, Academia institutions such as university libraries, to embed interview results in literature	Online data	Online databases
5. Views of cybersecurity professionals: Responses to COVID-19 cybersecurity crisis, future production and preparedness, suggestions for improvements, etc.	Qualitative data and online data	Responses from 30 semi-structured interviews

Source: Researcher's own

3.5. Target population and sample strategy

During the qualitative study, the researcher had the option to choose from three different sampling techniques: theory, convenience, or judgement (Marshall, 1996). The convenience sampling method was found to yield less precise results due to the researcher's aim to reduce study time and cost (Neuman, 2014). The theoretical sampling method was commonly used in a grounded theoretical approach, involving iterative sampling, analysis, and testing against a specific hypothesis. The judgement sampling technique, also known as purposive sampling, was widely used due to the researcher's deep understanding of the research topic, relevant literature, and the study itself (Patton, 1987).

The study utilised purposive selection to select cybersecurity professionals with extensive knowledge to gauge the impact of COVID-19 on organisational cybersecurity. Their proficiency was crucial in understanding the challenges encountered by organisations, the

vulnerabilities that emerged during the pandemic, and the measures taken to combat cyber-threats. The prevalence of remote work, online collaboration tools, and cloud-based solutions due to the COVID-19 outbreak compromising the cybersecurity status of organisations.

Cybersecurity professionals could provide critical insights concerning the issues they faced in securing their networks and data. During the pandemic, cyber-threats and attacks emerged, and the role of cybersecurity professionals was quintessential in managing and reducing these threats. It was imperative to conduct thorough interviews with these experts to comprehend the latest methods and antics employed by cybercriminals who targeted SA organisations during the pandemic, which triggered changes in attitudes and behaviours of employees, clients, and other cybersecurity stakeholders. Interviewing cybersecurity professionals would aid the researcher in comprehending human factors that influenced cybersecurity-threats and their evolution post-outbreak.

3.6. Research instrument

Conducting data collection using a deductive approach in qualitative research relies on having clear and distinguishable concepts (Hyde, 2000). The aim was to investigate the variables of the ATF that represented the concepts under exploration. It was crucial to have a proper understanding of the research topics before data collection began. Table 3.2 shows the themes derived from the ATF elements.

Table 3.2: Activity system elements study representations

Element	Element Definition	Themes
Activity	In the context of the Engeström Activity Theory framework, the primary activity to focus on for a study investigating the effects of COVID-19 on cybersecurity in organisations in South Africa was the "cybersecurity management activity" within the broader organisational context. The goal of cyber management activity was to ensure the confidentiality, integrity, and availability of an organisation's information and technology systems, as well as to mitigate potential risks and respond effectively to cybersecurity incidents.	The cyber security management activity encompasses various processes, practices, and systems implemented by organisations to protect their digital assets from cyber-threats. This includes activities such as risk assessment, development of cybersecurity policies and procedures, incident response planning, employee training and awareness programmes, regular monitoring and analysis of cyber-threats, and continuous improvement of security measures.
Subject	The Subject element refers to the individuals or groups actively engaged in the tasks and working towards achieving the object. These subjects are the participants or actors involved in the activity and play a central role in the system.	The subject was the 30 cybersecurity professionals who were engaged in the investigation and mitigation activities. They possessed the knowledge, skills, and expertise required to monitor, analyse, and respond to phishing attempts.
Tools	The Tools encompass the resources, technologies, and materials utilised to support and facilitate the activity. They can range from physical tools to digital platforms and knowledge resources. Tools play a crucial role in enabling individuals or groups to accomplish the objectives of the activity system.	Cybersecurity management tools common themes: Mimecast Phishing simulations Vulnerability scans EDR solutions Microsoft Defender Antivirus tools

Element	Element Definition	Themes
Community	The Community element recognises the significance of social interaction and collaboration within activity systems. It involves the formation of a community that facilitates knowledge-sharing, support, and coordination amongst the individuals or groups involved. The community provides an environment for collective learning and problem-solving.	Community common main theme 1: Implementation of policies. Community common main theme 2: Cultivating a cybersecurity-aware culture and environment.
Division of Labour	The Division of Labour element refers to the allocation of tasks and responsibilities amongst individuals or groups within the activity system. It recognises that different roles and expertise are necessary to achieve the objectives of the activity. This ensures efficient utilisation of resources and promotes specialisation in the system.	Division of labour common main theme 1: Comprehensive security controls, team processes and addressing skills scarcity. Division of labour common main theme 2: Efficient task allocation and responsibility-sharing.
Rules	The Rules refers to the guidelines, regulations, and procedures that govern the activity system. They provide structure, norms, and standards that dictate how the activity should be conducted. Compliance with these rules is vital for effective functioning and coordination within the system	Rules common main theme 3: Relevance of industry frameworks and standards.
Object	The Object is the action that is performed to achieve the outcome. The Object aligns with the activities of a cybersecurity management system by focusing on the actions employed by cybersecurity professionals. Key activities in a cybersecurity management system involve conducting risk assessments, deploying secure remote access solutions, enhancing employee awareness and training, and implementing incident response plans.	Object common main theme 1: Phishing simulation and awareness training. Object common main theme 2: Multi-factor authentication implementation. Object common main theme 3: Remote work adaptation. Object common main theme 4: Incident response plan adaptation. Object common main theme 5: Prioritisation of patching. Object common main theme 6: Policy development and enforcement.
Outcome	The Outcome is the transformative result of the subject's active engagement with an activity. The outcome element is closely tied to the object of the activity and serves as an evaluation of whether the intended goals have been achieved.	Outcome common main theme 1: Cybersecurity awareness. Outcome common main theme 2: Cyber-threats mitigation. Outcome common main theme 3: Cybersecurity advancements.

Source: Researcher's own

3.7. Research data collection method

Semi-structured interviews allow for a deeper understanding of subjective experiences and perspectives (Johnson & Christensen, 2017). The open-ended nature of these interviews enables participants to express themselves freely, providing rich and nuanced data. The flexibility and adaptability of semi-structured interviews allows for the analysis of unexpected topics or issues that may arise during the interviews. This flexibility ensured that the research remained responsive and adaptive to emerging themes or insights that were important to the participants. The semi-structured interviews allowed participants to share their thoughts, concerns, and challenges in their own words, ensuring that the data collected was grounded in their lived experiences. Building rapport and trust with participants was essential in semi-

structured interviews to encourage open sharing. Hence, establishing rapport and engagement facilitated a deeper level of analysis and understanding of the research topic (Johnson & Christensen, 2017).

3.8. Ethics

The researcher implemented measures to increase study participation while upholding ethical standards to ensure ethical conduct and maintain the organisation's integrity and reputation. Firstly, the researcher ensured participant anonymity, creating a secure environment for them to share their experiences and perspectives without fear of negative consequences. Secondly, the researcher received valuable feedback from diverse participants, resulting in a comprehensive and representative understanding of the topic under investigation due to the emphasis on increased participation. Thirdly, the researcher upheld ethical standards by obtaining informed consent, preserving confidentiality, and protecting participant identities, with transcripts and materials carefully crafted to maintain anonymity. Unique participant codes were assigned to everyone to safeguard their identities and maintain confidentiality during the analysis and reporting stages of the study. The researcher adhered to ethical protocols by obtaining authorisation to interview external cybersecurity specialists (Appendix B), ensuring participants were informed about the study's purpose, rights, and confidentiality measures.

3.9. Data analysis

In 2006, a comprehensive study was carried out using the widely recognised Braun and Clarke methodology for thematic analysis. The researcher analysed interview transcripts, ensuring an understanding of the data, resulting in the development of initial codes for subsequent analysis phases and substantiating themes with participants' personal experiences and statements, thereby providing valuable insights. Potential themes were identified by examining relationships and patterns within the codes. This analysis allowed for ongoing refinement and evaluation of themes through the merging or division of concepts as necessary. Finally, the researcher conducted a thematic analysis of the data, identifying and interpreting the underlying patterns and connections, making a significant contribution to the research field. This approach ensured that the final themes accurately reflected the overall concepts and ideas extracted from the data.

The study identified four key themes: COVID-19-related cybercrime types, vulnerabilities exposed, cybersecurity challenges faced by professionals, and cybersecurity strategies employed by these professionals.

3.10. An examination of the data

The researcher transcribed all interviews after conducting the initial interviews, allowing for the adaptation and modification of questions based on previous results, accelerating the process. The Braun and Clarke (2006) framework, which incorporates inductive and deductive reasoning in analysing qualitative data, was utilised and presented in Figure 3.2. To implement Ollerenshaw and Creswell's (2002) methodology, the researcher used NVivo, a qualitative data analysis program recommended by Saunders et al. (2009). The software enabled precise tracking of participant data sets, themes, quotes, and codes, using the Ollerenshaw and Creswell approach for methodical analysis to identify patterns, themes, and correlations. With the use of NVivo, various data types, including interview transcripts, field notes, papers, and multimedia, were efficiently and systematically processed as illustrated in Figure 3.2.

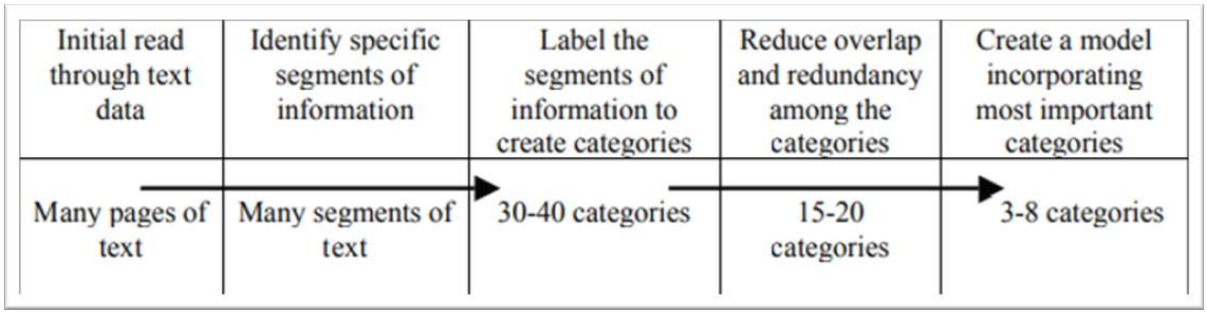

Figure 3.2: Modified version of Ollerenshaw and Creswell

Source: Ollerenshaw and Creswell (2002:266 – fig 9.4)

3.10.1 Step 1: Familiarising yourself with your data

The researcher conducted interviews to identify key ideas and phrases for further analysis, grouping them into themes to structure the raw data. The researcher continuously refined categories and subcategories to ensure understanding, detecting patterns of similarity, and incorporating new themes and concepts as they emerged. This phase was crucial in setting the groundwork for analysing the data further, as emphasised by various sources (Braun & Clarke, 2006; Vaismoradi et al., 2016; Rodgers & Cowles, 1993).

3.10.2 Step 2: Creating initial codes

Writing is a valuable tool for expressing ideas, identifying gaps in information, and guiding targeted investigations in research hypothesis development and theoretical framework development. Note-taking, a systematic and documented data analysis technique, can reduce researcher bias and enhance the recognition of subtle nuances in data, such as tone and nonverbal signs.

The study emphasises the importance of taking notes after transcription for a thorough qualitative data analysis, thereby enhancing the understanding of participants' experiences and viewpoints. The tool helped identify themes, codes, and theoretical frameworks, reduced researcher bias, and captured data complexities not easily distinguishable through transcripts or recordings (Braun & Clarke, 2006; Vaismoradi et al., 2016; Rodgers & Cowles, 1993). Coding was initiated and refined during the process (Figure 3.3).

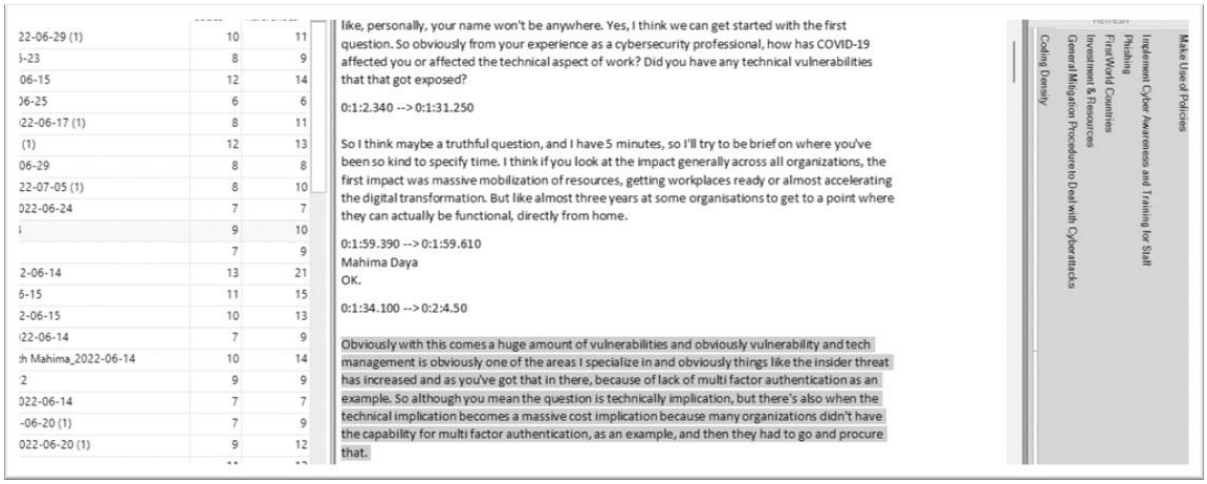

Figure 3.3: Development of coding

Source: Researcher's own

3.10.3 Step 3: Looking for themes

Historically, data analysis utilised the deductive method without focusing on classification, aiming to understand data by organising related codes and comprehending their complexity. The researcher utilised a deductive methodology to identify themes that directly addressed their research question, allowing a comprehensive exploration of the data's intricacies. The deductive method was used exclusively to identify and develop themes that aligned with the research objectives, accurately capturing the collected data (Vaismoradi et al., 2016; Braun & Clarke, 2006; Patton, 1987).

3.10.4 Step 4: Examining themes

Following the analytical process, the identified themes were refined and augmented to align with research objectives, ensuring relevance to the topic, and the data was sorted and scrutinised for a comprehensive analysis. The modifications made to the process of theme analysis proved to be beneficial in preserving the authenticity and significance of the study (Braun & Clarke, 2006; Maguire & Delahunt, 2017).

3.10.5 Step 5: Specifying and naming themes

Figures 3.4 and 3.5 depict the development of themes, emphasising the importance of understanding the underlying rationales that highlight their appeal or significance throughout the investigation. Scholars noted the interconnectedness amongst the themes and the potential existence of secondary or subsidiary sub-themes (Braun & Clarke, 2006; Vaismoradi et al., 2016). The assigned appellations for each theme should be informative and straightforward, ensuring research continuity without ambiguity.

Figure 3.4: Modified version of Braun and Clarke

Source: Braun and Clarke (2006:21 – fig. 6)

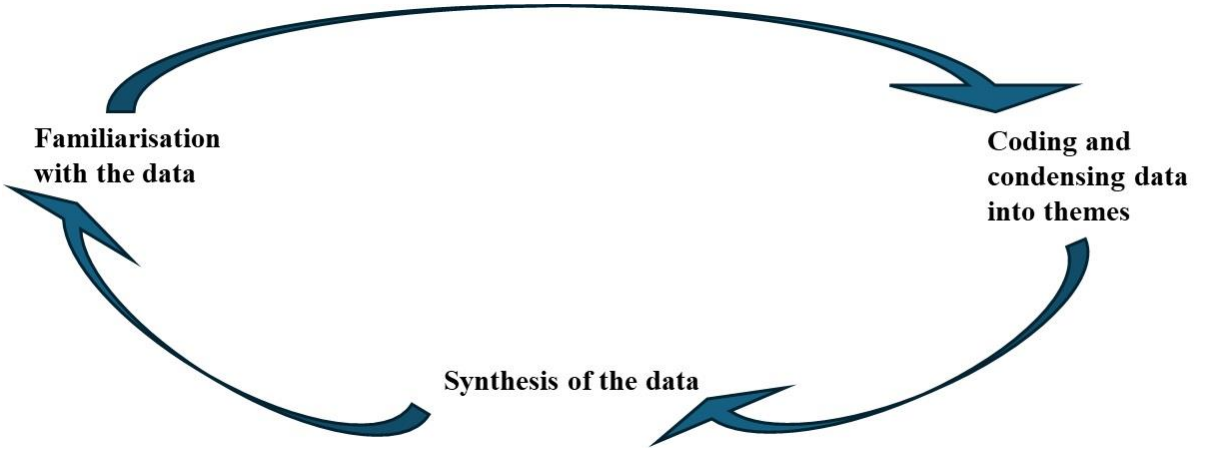

Figure 3.5: Development of coding

Source: Researcher's own

3.10.6 Step 6: Creating the report

In accordance with Braun and Clarke's (2006) recommendation to create a concise and precise report without using overused phrases, a narrative analysis of the dataset was conducted to validate the credibility of the data segments linked to the prevalent topics. To ascertain their reliability, a brief and methodical inquiry was executed. As a result, the definitive document recorded the outcomes of this approach (Braun & Clarke, 2006).

3.11. Tools used

The researcher conducted a preliminary analysis using Microsoft Word and Excel, followed by a comprehensive analysis using NVivo software to identify key correlations or codes. The study's rigour and quality were enhanced by combining manual and NVivo analyses, enabling a more comprehensive examination of the data. However, the researcher faced difficulties in analysing underlying themes due to the lack of semantic processing in NVivo software.

Bhattacherjee (2012) emphasised caution when using multiple software programs in data analysis, citing the increased likelihood of errors and the difficulties in organising information. Using popular data analysis programs could lead to misunderstandings of data as well (Bhattacherjee, 2012). Pickard (2007) recommends consistent record-keeping for data accessibility. The researcher organised data in NVivo and digital files, creating backup copies in Microsoft OneDrive for accurate preservation.

3.12. Research project plan

The researcher planned and composed each chapter of their Master's Dissertation from April 2023 to June 2024, starting with background research, research questions, and objectives. Next, they gathered literature for Chapter 2, followed by designing the research methodology for Chapter 3 and conducting data collection and analysis. The researcher then drafted and refined each chapter, presented findings in Chapter 4, discussed them in Chapter 5, and concluded by submitting the final draft for evaluation. Table 3.3 shows the timeline breakdown of tasks per chapter.

Table 3.3: Dissertation Timeline

Timeline	Task
April 2023	Begin background research for Chapter 1 (Introduction)
May 2023	Develop research questions and objectives for Chapter 1
June 2023	Start drafting Chapter 1
July 2023	Continue refining Chapter 1 and seek feedback
August 2023	Start gathering literature for Chapter 2 (Literature Review)
September 2023	Analyse and synthesise literature for Chapter 2
October 2023	Begin drafting Chapter 2
November 2023	Continue refining Chapter 2 and seek feedback
December 2023	Finalise Chapter 1 and Chapter 2
January 2024	Design research methodology for Chapter 3 (Research Methodology)
February 2024	Begin data collection and analysis for Chapter 3
March 2024	Draft Chapter 3
April 2024	Continue refining Chapter 3 and seek feedback
May 2024	Present findings in Chapter 4 and start on Chapter 5 (Findings and Discussion)
June 2024	Finalise Chapter 4 and Chapter 5, and work on Chapter 6 (Conclusion)
June 2024	Complete final draft of the Dissertation, including all chapters, and submit for evaluation and assessment

Source: Researcher's own

3.13 Chapter 3 Summary

Chapter 3 outlines the research methodology employed in this study, detailing the research philosophy, epistemology, and ontology that underpin the analysis of cybersecurity experts' experiences during the COVID-19 pandemic. The chapter discusses the deductive thematic analysis adopted, which allows for movement from a conceptual model to identify themes using the predictions of that model. This approach emphasises the subjective perspectives of participants while ensuring structured analysis. A pragmatic paradigm stance is indicated, permitting the use of both qualitative and quantitative methods. The chapter delineates the research purpose, time framework, data requirements, sampling strategy, and ethical considerations involved. Additionally, it describes the data analysis process, tools utilised, and the timeline of the research project. Overall, it provides a comprehensive overview of the methodological framework guiding the investigation into the effects of COVID-19 on cybersecurity practices in South African organisations.

Chapter 4: Findings and discussion

The study employed thematic analysis, following the method outlined by Braun and Clarke, (2006) to delve into the realm of cybersecurity management practices in SA organisations during the pandemic. The study identified key themes under the elements within the cybersecurity management strategies, based on existing literature and academic theories.

4.1 Ensuring the reliability of research findings

The researcher practiced reliability, accuracy, and dependability of the research findings using a structured approach involving member-checking to authentically capture the cybersecurity professionals' experiences. Member-checking is a validation technique necessary for credible qualitative research. It helped verify the findings with participants to ensure data accuracy and credibility, sharing key findings and seeking feedback (Motulsky, 2021). An audit trail was crucial for transparency, accountability, and independent verification of research steps, enhancing the credibility of the study (Carcary, 2009). Thus, the researcher's reflexivity and critical stance were instrumental in ensuring objectivity, rigour, and trustworthiness of their findings, by acknowledging and addressing their own positionality (Shufutinsky, 2020).

4.2 Validating the study's findings

The study ensured internal validity through structured interviews, promoting candid responses, reducing biases, and building trust with participants to enhance credibility. The research context was detailed to highlight SA organisations' unique challenges during the pandemic, and its reliability was ensured through reflexivity. Reflexivity in research involves being aware of and actively considering one's own biases and assumptions to ensure accurate findings (Darawsheh, 2014). The study's findings were confirmed through direct quotes and participant validation, ensuring accurate representation of participants' unique perspectives and experiences. Table 4.1 provides information pertaining to the 30 participants.

(Some information such as participant name, age and the organisations' names could not be disclosed due to confidentiality agreements).

Table 4.1: Consolidated table of participants' data

Participant number	Profile	Sex	IT Experience in years	Cybersecurity experience in years	Company size (number of employees)	Cities	Industry sector	Education	Certifications / Skills / Licenses
P1	Acting head of IS governance	Female	16+	6+	50+	Johannesburg, Pretoria	Technology/Software	Business School Certificate, Strategic thinking and execution for growth- Senior Management Development Programme- GIBS Business Competence Certificate, Business Administration and Management, General- Bachelor's Degree, Information Systems- Bachelor's Degree, Management Information Systems, General	COBIT 2019 Foundations certificate, Management Information Systems, General- ISO27001 Foundations Certificate, Computer and Information Systems Security or Information Assurance- Certified Information Security Manager (CISM), Information Security- ITIL Foundations, Information Technology
P2	Cybersecurity engineer	Male	11+	6+	10,000+	Bloemfontein	Education	BCom Industrial Psychology and Labour Relations Management from North-West University- Studied Accounting, Afrikaans, Computer Science, English, Mathematics, and Physics at Secunda High School.	Skills in Network Security and Firewalls- IELTS Academic and IELTS Official qualifications- Regulatory Exam 5 certification- Check Point Certified Security Administrator (CCSA R81); Completed a Short Course in Cybersecurity at the University of Pretoria.
P3	Cybersecurity consultant	Male	5+	5+	50+	Johannesburg, Pretoria	Technology/Security	BS (Hons), Mathematics from University of Cape Town - Bachelor of Science - BS, Mathematics and Computer Science from University of Cape Town	Skills: Hacking · Ethereum · Smart Contracts · Bug bounty as an Independent Security Researcher
P4	Deputy director: protection services	Female	11+	11+	10+	Johannesburg, Pretoria, Cape Town	Technology/Security	University of Pretoria: Short Course in Policy Management, Implementation, and Analysis in the Public Sector, Public Management- MANCOSA: Master of Business Administration (MBA), Business Administration and Management, General- MANCOSA: Postgraduate Diploma in Business Management, Business Administration and Management, General- University of Cape Town: Certificate in Project Management- University of the Witwatersrand: Master of Management, Security- University of Cape Town: Certificate in Fundamentals of Cybersecurity- University of Pretoria: Short Course in Information Security Management- University of the Witwatersrand: Postgraduate Diploma in Management (Security), Security Management- University of Johannesburg: BA Psychology, Humanities	IELTS Academic certification- IELTS Official certification- Regulatory Exam 5- Financial Planning Institute SA certification- Check Point Certified Security Administrator CCSA R81 certification- PSiRA certification- Skills: Security Operations- SSA or NIA Security Man- Skills: Vulnerability Assessment- 11 years in cyber and tech experience
P5	Cybersecurity and technology risk consultant	Male	21+	10+	50+	Johannesburg, Cape Town, Durban	Technology/Security	University of Cape Town: Master's degree, Information Systems - Midlands State University: Bachelor of Science (Honours) Degree, Information Systems	Microsoft Azure Security Technologies (AZ-500) Cert Prep: 3 Manage Security Operations - Certified Information Security Manager (CISM)
P6	Cybersecurity consultant	Male	7+	7+	10+	Johannesburg, Pretoria, Cape Town	Technology/Security	Stellenbosch Business School: Management Development Programme - Cape Peninsula University of Technology: Master of Technology - MTech, Computer and Information Systems Security or Information Assurance	CBM Training - Report Writing Skills - Certified in Cybersecurity - $(ISC)^2$
P7	Cybersecurity specialist	Male	3+	3+	10+	Johannesburg, Pretoria, Cape Town	Technology/Security	Durban High School Qualification	- Offensive Security Exploit Expert - Offensive Security Wireless Expert - Offensive Security Web Expert - Linux Privilege Escalation - Windows Privilege Escalation - Web Application Security and Testing - Mobile Application Penetration Testing - Practical Malware Analysis & Triage - Solutions Architect Associate, Amazon Web Services - Open Source Digital Forensics Examiner - Offensive Security Certified Professional - Android Mobile Forensics (W36) - Advanced Open Source Intelligence and Privacy - Open Source Intelligence - Website Security - CEH v10 - Linux Forensics - Mobile Ethical Hacking -
P8	Cyberdefence incident responder	Female	15+	15+	50+	Johannesburg, Pretoria	Education/Technology/Security	Bachelor of Science - BS in Cyber Security from IU International University of Applied Sciences	Accreditations and qualifications for: Response center specialties; Network engineering; Client, Systems, Integrity and Compliance Administrator and Trainer; Customer services analyst – Contractor; Cyber security analyst; Incident Response Practitioner

Participant number	Profile	Sex	IT Experience in years	Cybersecurity experience in years	Company size (number of employees)	Cities	Industry sector	Education	Certifications / Skills / Licenses
P9	Director	Female	21+	21+	10,000+	Johannesburg, Cape Town, Durban	Retail/Fashion	Holds a PhD in Computer Security from the University of South Africa- Holds a BSc in Computer Science, a BSc Honns in Statistics, and an MSc in Computer Science from North-West University- Holds a BSc	PhD in mobile agent security, guiding global and industry research projects, extensive publications, keynote speaker, panellist on cyber-crime, cyber warfare, cyber intelligence, Adjunct Professorship, Extraordinary Associate Professorship, expertise in cyber intelligence, cyber warfare, nano-satellite security, cyber security capacity building, skill development, forensic analysis, cyber warfare tactics, cyber investigations, criminology, penetration testing, governance.
P10	Cybersecurity executive consultant	Male	17+	7+	100+	Johannesburg, Cape Town, Durban, Pretoria, Gqeberha	Technology/Consulting	Bachelor of Commerce (BCom) from the University of Stellenbosch	Azure Fundamentals Certified- CISSP by (ISC2)
P11	Security solutions architect	Male	13+	7+	10,000+	Johannesburg, Cape Town, Durban	Energy/Petroleum	Stellenbosch Business School: Management Development Programme - Cape Peninsula University of Technology: Master of Technology - MTech, Computer and Information Systems Security or Information Assurance	CBM Training - Report Writing Skills - Certified in Cybersecurity - (ISC)²
P12	IT delivery manager in cybersecurity	Male	8+	7+	10,000+	Johannesburg, Cape Town, Durban, Pretoria	Retail/Food and Beverage	BCOM in Management Information Systems from the University of Western Cape	PRINCE2® Foundation and Practitioner Certification Training- Certified SAFe® 5 Scrum Master
P13	Head of research development and innovation in cybersecurity	Male	15+	15+	10+	Johannesburg, Pretoria, Cape Town	Technology/Security	Rhodes University: Master of Science (MS), Computer Science - University of Pretoria: B.IT, Computer Science, Information Technology, Informatics, Multi-media, Information Science	Oracle Cloud Infrastructure 2021 Certified Cloud Operations Associate- Oracle Cloud Infrastructure Foundations 2021 Associate- Oracle Cloud Infrastructure Security 2021 Certified Associate- Oracle Cloud Platform Identity and Security Management 2021 Certified Specialist- Machine Learning Advanced Certification- Microsoft Certified: Identity and Access Administrator Associate- Microsoft Certified: Security Operations Analyst Associate- SentinelOne Partner Tech Accreditation 101- Microsoft Certified: Security Operations Analyst Associate
P14	Cloud penetration tester	Male	5+	5+	10,000+	Johannesburg, Cape Town, Pretoria, Durban, Gqeberha, Bloemfontein	Financial Services	Master of Commerce (MCom.) in Information Systems, Rhodes University- Bachelor of Commerce (BCom) with Honors in Information Systems, Rhodes University- Bachelor of Commerce (BCom) in Information Systems and Management, Rhodes University	Attacking and Defending Azure AD Cloud - Pentester Academy- Microsoft Azure Security Engineer- Systems Security Certified Practitioner (SSCP) (ISC)²
P15	Cybersecurity engineer	Male	12+	5+	200+	Johannesburg, Pretoria	Technology/Software	Not provided	Autopsy Online Training (Autopsy Basics and Hands-On)- CyberArk Trustee- ISTQB - Certified Test Analyst- Agile Bootcamp- Microsoft Certified Azure Security Engineer- Microsoft Azure Fundamentals
P16	Information officer / Security engineer	Male	26+	26+	5,000+	Johannesburg, Cape Town, Durban, Pretoria	Technology/Software	University of Cape Town: Fundamentals of Cybersecurity online short course - University of Cape Town: Data Protection and Privacy online short course	Associated Professional Member (APM) - ISACA South Africa Chapter - Information Officer - Information Regulator (South Africa) - Data Privacy - Private Security Industry Regulatory Authority - Grade A (PSiRA)
P17	Cybersecurity specialist - blue team	Female	2+	2+	500+	Johannesburg, Cape Town, Durban	Telecommunications	Bachelor of Science Honours in Computer Science from University of Cape Town - Bachelor of Science in Computer Science & Business Computing from University of Cape Town	CompTIA Security Certification - SAP ERP Certificate of Proficiency
P18	Senior IT security engineer	Male	6+	6+	500+	Johannesburg, Cape Town, Pretoria	Technology/Software	Postgraduate Diploma in Project Management (MANCOSA)	Certified Arcsight Admin and Analyst
P19	Senior technical specialist (information and cybersecurity services)	Female	7+	Not specified	5,000+	Cape Town	Education	Bachelor of Commerce - BCom (Hons), Information Systems from the University of Cape Town- Postgraduate Diploma in Digital Computer Forensics with BCom (Hons) Information Systems from the University of Cape Town	Cybersecurity Awareness Training (ESET North America)- Microsoft Certified Systems Engineer: Windows Server 2003 (MCSE) (Microsoft)- CompTIA A+ (CompTIA)- Certified Ethical Hacker (CEH) (EC-Council)- Foundations of IT Security: Network Security (Lynda.com)- Foundations of IT Security: Core Concepts (Lynda.com)

Participant number	Profile	Sex	IT Experience in years	Cybersecurity experience in years	Company size (number of employees)	Cities	Industry sector	Education	Certifications / Skills / Licenses
P20	Information security analyst	Male	4+	3+	200+	Johannesburg, Cape Town, Durban, Centurion, Gqeberha, Pretoria, Bloemfontein, East London, Pietermaritzburg, Polokwane, Rustenburg	Technology/Fintech	Higher Certificate Information Technology (User Support Service) from Nelson Mandela Metropolitan University - Diploma in Information Technology from Nelson Mandela University	Certified in Cybersecurity (ISC2) - CompTIA Security+ ce Certification - (ISC2) Candidate - Microsoft Technology Associate: Security Fundamentals
P21	Cybersecurity manager	Male	6+	2+	14,000+	Johannesburg, Pretoria, Cape Town, Durban	Professional Services/Accounting	Bachelor's Degree (Honours), Information Technology from University of KwaZulu-Natal - Bachelor's Degree, Computer Science and Information Systems and Technology from University of KwaZulu-Natal	Certified Information Systems Auditor (CISA) - ISACA - COBIT 5 Foundation - Azure Fundamentals - Microsoft
P22	Senior specialist: IT security	Male	11+	11+	1,000+	Bloemfontein, Pretoria	Financial Services	Tshwane University of Technology - Bachelor of Technology, Information Technology- University of Johannesburg - Information Management, Information Technology	Certified Information Security Manager® (CISM)- IT Information Library Foundations Certification (ITIL)- Introduction to Information Security- Principles of Information Security
P23	Senior cybersecurity consultant	Male	15+	10+	500+	Johannesburg, Durban	Healthcare	Information Technology Qualification from Intuition College	Certified in Cybersecurity (CC) - $(ISC)^2$
P24	IT governance, risk and compliance manager	Female	13+	2+	10,000+	Johannesburg, Durban	Food and Beverage	Postgraduate Degree, Business Management - University of KwaZulu-Natal: BCom Information Systems & Technology and Supply Chain Management, Information Technology	ITIL Foundation in IT Service Management, AXELOS Global Best Practice - Certified Information Systems Auditor, ISACA South Africa Chapter
P25	IT governance and security analyst	Female	6+	4+	10+	Johannesburg, Cape Town, Durban, Pretoria	Technology/Software	Doctor of Philosophy - PhD, Information Systems: University of Cape Town	Microsoft Certified: Security, Compliance, and Identity Fundamentals
P26	IT security analyst	Male	7+	7+	10,000+	Johannesburg, Pretoria, Cape Town, Durban	Financial Services	National Diploma in Information Technology from Walter Sisulu University of Technology- BTech Information Technology in Communication Networks from Walter Sisulu University of Technology (2016 - 2016)	Fortinet Network Security Expert Level 1: Certified Associate- Fortinet Network Security Expert Level 2: Certified Associate- Fortinet Network Security Expert Level 3: Certified Associate- Cobit 5- CompTIA Security+- Mimecast Gateway Technical Professional (Expired)- Mimecast Gateway Technical Specialist (Expired)- Certified Ethical Hacker (CEH)- IT Information Library Foundations Certification (ITIL)- O365 Security Administrator
P27	Cybersecurity senior analyst	Male	5+	5+	200+	Johannesburg, Cape Town	Technology/Security	Bachelor of Science - BS, BSc. Computer Science from University of the Western Cape	$(ISC)^2$ Candidate; Master Cybersecuirty Management; Practical cybersecurity for IT Professionals; CompTIA PenTest Certification CompTIA
P28	Cybersecurity manager	Male	7+	7+	200+	Johannesburg, Cape Town, Durban, Pretoria	Financial Services	BBA in Business Administration from Global Business School - BBA & BCA (Bachelor of Business Administration and Bachelor of Computer Applications) from Global Business School	Intel Security VirusScan Enterprise 8.8 - McAfee - Intel Security ePolicy Orchestrator 5.1 - McAfee
P29	Cybersecurity manager	Male	5+	5+	5,000+	Bloemfontein, Cape Town, Durban, East London, eMalahleni, Middleburg, Kimberley, Mahikeng, Pietermaritzburg, Gqeberha, Robertson, Stellenbosch, Worcester	Professional Services/Accounting	Bachelor of Science (BS) in Computer Science from the University of the Western Cape	Microsoft Certified: Azure Fundamentals- CSX Cybersecurity Fundamentals Certificate (CSXF)- Certified Ethical Hacker (CEH)
P30	Software engineer	Male	7+	7+	200+	Cape Town	Financial Services	Honours in Computer Science from the University of Cape Town	Java from TestDome

Source: Researcher's own

4.3 Preliminary assessment

To provide a deeper understanding of the activity theory elements, the researcher conducted a preliminary assessment of the study. The assessment aimed to identify key themes, patterns,

and relationships that would inform and contextualise the analysis of the other elements in this section later.

4.3.1 Theme 1: Vulnerability assessment

Participants highlighted which industry was most susceptible to cybersecurity-threats during the pandemic. According to participant P3, a cybersecurity consultant working in the technology and security industry based in Johannesburg and Pretoria stated:

> *"I couldn't really say if there was a particular company that was affected, but just overall in the space, there's been a lot of threat actors."*

This suggests that the entire cyberspace, rather than specific companies, has been exposed to an increased number of cyber-threats.

Participant P5, a cybersecurity and technology risk consultant in a company with branches in Johannesburg, Cape Town, and Durban, further emphasised that:

> *"SA is regarded as an economic powerhouse - a lot of international companies operating in SA, for an organisation to be vulnerable to attacks, it doesn't necessarily need to be in any country, but it also depends on the type of information or the type of business you are into."*

They went on to explain that cybercriminals have a motive, citing examples such as data being *"the new oil and corporate espionage"*.

Participant P13, a head of research development and innovation in cybersecurity, with their organisation operating in Johannesburg, Pretoria, and Cape Town, noted that:

> *"I wouldn't say it's a specific industry or type of business that has been attacked - but everything at the moment, I've seen lots of weird combinations."*

This shows that cybercriminals are targeting a wide range of industries and organisations.

In contrast, participant P14, a cloud penetration tester in the financial services industry, representing branches in Johannesburg, Cape Town, Pretoria, Durban, Gqeberha, and Bloemfontein, noted that:

> *"The financial institutions and governments are mostly affected from cybercrime - it was a bit more, especially during the Russian-Ukraine war."...."Cyber-threats had*

increased slightly more during the COVID-19 period; and by that - when you're looking at cybercrime, they're different levels of cyber criminals".

Participants P21 and P29 highlighted the importance of government institutions and data centres being targeted by cybercriminals. Participant P21, a cybersecurity manager working in the professional services in the accounting industry and based in Johannesburg, Pretoria, Cape Town, and Durban, stated that:

"Most attacks now, I believe, target government institutions, they know what attacks are typically used when they see that most companies are vulnerable in this particular environment or in this prosperous country".

Participant P29, a manager in cybersecurity working in professional services and accounting, with branches in Bloemfontein, Cape Town, Durban, East London, eMalahleni, Middleburg, Kimberley, Mahikeng, Pietermaritzburg, Gqeberha, Robertson, Stellenbosch and Worcester noted that:

"Data centres play a crucial role in housing various services for organisations. These data centres may be located in India, Australia, the United States, or any other country. If a SA organisation's data is hosted in these data centres, it could have an impact."

Based on these findings, the convergence of motivated offenders (cybercriminals) and suitable targets (financial institutions and governments) increases the likelihood of criminal activity occurring when there is a lack of capable guardians (adequate security measures) (Clarke & Felson, 1993). In this context, the increasing presence of threat actors, SA's attractiveness to cybercriminals, and vulnerability across industries create a conducive environment for criminal activity. Thus, the lack of capable guardians, such as inadequate security measures, allows these crimes to go unpunished.

4.3.2 Theme 2: Digitisation

The analysis of participant responses revealed a consistent pattern of concern regarding the catalyst that triggered the increased focus on cybersecurity, specifically the COVID-19 pandemic and the rapid digitisation that accompanied it. Participant P22, a senior specialist in IT security, employed in an organisation with over 1,000 employees, emphasised that:

"I think it was more the digitisation of organisations because, I mean COVID-19 was there, it was just people were trying to figure out how to operate under the new normal. So they move to the digital realm and because of that, like I said earlier, they adopted

a whole bunch of new software tools, processes, but they didn't really consider security elements, because it generally takes longer if you do that and they want it to get up and running as quick as possible. So they digitised, but they don't really secure - it was more on the digitisation of processes to make sure people still had access to things."

This sentiment is echoed by existing literature, which highlights the importance of organisations adapting security measures to the remote work environment (Boughrous et al., 2021). This is in line with the concepts of Social Disorganisation Theory (SDT), which suggests that disruptions in the social structure, such as the rapid shift to remote work, can lead to an increase in crime and deviant behaviour (Shaw & McKay, 1942). For example, in the context of multi-factor authentication (MFA) implementation and remote work, these disruptions could have created new opportunities for cyber-threats and attacks, requiring organisations to adapt security measures, maintain processes, and address vulnerabilities to prevent security breaches.

Participant P23, a senior cybersecurity consultant in a 500-person organisation, said:

"*Definitely digitisation - There was a shift with companies moving or needing to move to a remote workforce and I think all the way through, from like 2020, when COVID hit, till now, we are still actually seeing that companies are utilising that work from home model. Somewhere you go, maybe 50% of your time is spent in the office, and the rest of the time is spent working remotely. We were already geared up for COVID remote work as an IT technology provider. For others, yes, we were busy helping them get remote, which allows them to become remote workers."*

This observation is consistent with literature that discusses the challenges of balancing security and speed during the swift adoption of new technologies during the pandemic (He et al., 2021). The literature supports participant P24's perspective by incorporating elements of Social Theory (ST), which suggests that organisations may have prioritised speed and efficiency over security measures in the face of rapid digitalisation due to stress and strain (Merton, 1936). This trade-off could have resulted in vulnerabilities that cyber-attackers could exploit.

4.3.3 Theme 3: Incident scenario identification and analysis

Regarding possible incident scenarios and tracking phishing trends to strengthen cybersecurity measures, the participants provided their first-hand experiences and viewpoints on the prevalent cybersecurity challenges during the pandemic. Their insights have been instrumental in showcasing the necessary actions to tackle evolving threats and vulnerabilities. Due to the sensitive and confidential nature of the attacks, participants were unable to disclose specific

details regarding other types of cybercrime, including data breaches, distributed denial-of-service (DDoS) attacks, and extortion attempts.

4.3.3.1 Sub-Theme 3.1: Increase in phishing attacks

The COVID-19 pandemic has led to a significant increase in cybercrime, with participants in the study highlighting the rise of phishing attacks as a major concern. According to participant P1, *"Cybercrime, has increased as a whole."* This was because the pandemic created an environment where individuals were more susceptible to cyber-attacks, as they were more likely to engage in risky behaviour in pursuit of financial or emotional support. Participant P7 said: *"There were a lot more cybercrime cases throughout the COVID times."* Participant P8 remarked that: *"The phishing things are almost like a daily occurrence, especially during 2021."* This showcased that the frequency and persistence of these attacks created a sense of urgency and vulnerability amongst individuals.

Participant P2 noted that phishing attacks were particularly effective during the pandemic, mentioning that:

> *"Falling for a phishing attack is not just going to give me access to your whole network - There were many layers of security that had to be overcome to breach a company, phishing worked so well once they got through the perimeter."*

Many participants highlighted the ease with which individuals were targeted by phishing emails. Participant P4 mentioned that: *"People were an easy target when it came to phishing emails".* Participant P6 added: *"Many SA websites lacked HTTPS encryption, making it easier for hackers to intercept data."* Thus, the lack of encryption and the ease with which individuals were targeted by phishing emails made it a prime target for cybercriminals.

The participants' insights can be explained by the theory of RCT (Morrison, 2022). According to this theory, individuals make decisions based on their subjective probability of success and the potential benefits of their actions. In the context of phishing attacks, individuals may be more likely to engage in risky behaviour if they perceive the benefits to be high (for example, financial gain or access to valuable information). The pandemic may have created an environment where individuals are more susceptible to these types of rational choices, as they may be more desperate for financial or emotional support.

4.3.3.2 Sub-Theme 3.2: Increase in social engineering attacks

The COVID-19 pandemic has led to a surge in social engineering attacks, which have become a significant concern for organisations. A thematic analysis of participant experiences and

existing literature on cybercrime trends during times of crisis has established the common theme of an increase in social engineering attacks. Participant P5, with over 21 years' IT experience, including 10 years' cybersecurity experience, noted that:

> *"We've witnessed a lot of social engineering attacks, especially business email compromise."*

This observation aligns with research that has found an increase in these attacks during the pandemic (Chigada & Madzinga, 2021). Social engineering attacks involve cybercriminals exploiting human vulnerabilities, such as trust and urgency, to manipulate individuals into divulging sensitive information or performing unauthorised actions (Momoh et al., 2023).

Participant P6, with over seven years' IT and cybersecurity experience, recounted an episode where trust was exploited using the chief executive officer (CEO)'s wife's Gmail account, stating that: *"Some incidents involved phishing emails or social engineering."* This incident exemplifies the underlying principles of the Social Learning Theory (SLT), which suggests that individuals may be influenced by observing those in positions of authority (Bandura, 1977). In this case, the cybercriminal targeted the CEO's wife's email account to gain unauthorised access, leveraging the trust associated with their relationship. The SLT highlights the importance of understanding how individuals learn and adopt behaviours, including those related to cybersecurity. To address social engineering attacks, the Social Cognitive Theory (SCT) provides insights into individual factors that influence behaviour change (Bandura, 1989). The SCT emphasises self-efficacy - an individual's belief in their ability to perform a specific behaviour. Thus, enhancing employees' self-efficacy in detecting and mitigating social engineering attacks is vital to preventing such incidents.

Education and awareness programmes play a crucial role in building self-efficacy and empowering individuals to recognise and respond effectively to social engineering tactics (Mahanta & Maringati, 2023). By providing employees with knowledge about common social engineering techniques, the consequences of falling prey to such attacks, and strategies for vigilance, organisations can enhance their ability to identify and mitigate potential risks.

4.3.4 Theme 4: COVID-19-themed incidents

The common theme of COVID-19-themed incidents was identified through a series of cybersecurity breaches and incidents reported by participants at the height of the pandemic, showcasing the specific targeting and exploitation of pandemic-related vulnerabilities.

According to participant P8,

> *"There had been a spike in spam and phishing attacks with a COVID-19 theme, taking advantage of people's heightened desperation during the pandemic."*

Participant P9 noted that they *"Saw a sort of spike in spam and phishing attacks with a COVID-19 theme."* This suggests that cybercriminals took advantage of the pandemic by using COVID-19-themed emails and messages to trick individuals into revealing sensitive information and capitalised on the public's heightened emotions and fears surrounding the pandemic, launching targeted attacks that exploited vulnerabilities.

Participant P24, with auditing and compliance experience, noted that*:*

> *"The number of threat-related incidents logged in our SOC had increased during COVID-19. Hackers exploited the lack of additional security measures when people worked from home."*

As a result, vulnerability of remote workers was exposed, often leaving them without adequate security measures to protect themselves against cyber-attacks.

Participant P27, with penetration testing (PenTest) skills, further discussed how:

> *"COVID-19 information was used to lure victims in phishing attacks. There was a spike in cyber-attacks, but organisations were learning from each other to stay ahead."*

This indicates that organisations were adapting to the changing threat landscape by sharing knowledge and best practices to stay ahead of emerging threats.

Participant P29, with skills in ethical hacking, shared that:

> *"Malicious actors posed as COVID-19 officials to gain access to buildings - people fell for COVID-19 related threats."*

Participant P20 added that:

> *"Emails enticed people to click, download software, read articles, follow links because there's a bit of sensation, around COVID-19 so attackers can generally leverage off that."*

This demonstrates the cunning nature and adaptability of cybercriminals, who can easily take advantage of crisis situations to further their malicious goals. As a result, these insights align with research findings that have shown a significant increase in COVID-19-themed phishing

attacks during the pandemic (Minnaar, 2020). Cybercriminals are leveraging people's fears and anxieties surrounding COVID-19 to deceive them into falling for malicious schemes.

4.4 Subject element

This study analysed 30 SA cybersecurity professionals to understand the effects of COVID-19 on their work (Table 4.1). The participants, including cybersecurity engineers and consultants, had diverse roles and varied levels of experience in IT and cybersecurity. They were located in various cities across SA, demonstrating broad geographic representation.

Working across industries like technology and finance, they offered perspectives on cybersecurity challenges across sectors. The organisations they worked for ranged in size from small businesses with 10 employees to large corporations with over 10,000 employees, showing diverse organisational sizes and cybersecurity needs. Participants held bachelor's and master's degrees with certifications from institutions like the International Information System Security Certification Consortium (ISC2) and the Computing Technology Industry Association (CompTIA). They specialise in areas like network security, compliance, incident response, penetration testing, and cloud security, with advanced certifications like Certified Information Security Manager (CISM) and Certified Ethical Hacker (CEH), showcasing expertise.

4.5 Tools element

The interview participants provided a diverse range of tools and technologies used in their cybersecurity management practices. The variety of tools and technologies used indicated a comprehensive approach to cybersecurity management across different sectors and organisations represented by the participants. Due to COVID-19 restrictions, these professionals relied on remote access tools and collaboration platforms to effectively manage and monitor cybersecurity systems in a remote working environment, within the cybersecurity management activity. To safeguard organisations against cyber-threats, it was crucial to implement a comprehensive cybersecurity strategy.

A range of tools were available to help prevent and detect attacks, including Mimecast, phishing simulations, and vulnerability scans. These tools were supplemented by advanced threat detection and response capabilities offered by endpoint detection and response (EDR) solutions and Microsoft Defender, while antivirus tools continued to play a vital role in providing real-time protection against malware and other types of threats. For a comprehensive

overview of the various cybersecurity tools that can be used to enhance an organisation's cybersecurity posture, see Table 4.2.

Table 4.2: Consolidated table of tools used

Participant Number	Cyber Management Tools
P1	1. Microsoft Suite 2. Yammer 3. Phishing ER 4. Phishing Simulations 5. Preventative controls 6. Monitoring tools 7. Early detection systems 8. Monitoring tools for network and device scanning 9. Tools for scanning outgoing and incoming data to prevent data leakage 10. Data loss prevention software 11. Phishing capability tool 12. Incident response process tool
P2	1. Conference Talks 2. Blog Posts 3. Pairing with Blue Team to Bring Awareness 4. Pickup Tool
P3	1.Bug run (bug hunting to find vulnerabilities)
P4	1. Minecast 2. Mankas Security Awareness Platform 3. USB port blocking policy 4. Official USB (UFD) provision 5. Microsoft 365
P5	1. KnowBefore 2. Phishing Simulations 3. Benchmarking and Targeted Training 4. Log Collection, Aggregation, and Correlation Systems (like SIM) 5. NOB4 (Cybersecurity Awareness tool) 6. Managed SOC (Managed Security Operating Center) 7. EDRs (Endpoint Detection and Response) 8. Parameter Firewall
P6	1. Purple teaming exercises 2. Triple T (Test, Train, short 5 min video with quiz, target them through purple team testing) 3. Logon Tracer 4. Zeek (formerly known as Bro) 5. Zeek technology (used by companies like Co Light and Dark Trace) 6. Sysmon (part of the sysinternal suite by Microsoft)
P7	1. manual techniques, such as using Boolean searches 2. Forensic acquisitions.
P8	1. User education 2. Talking one on one 3. WhatsApp (as a communication tool) 4. Different tools from different vendors (for cybersecurity purposes)
P9	1. Programmer's source 2. Newsletters, writings, and blogs 3. Virtual training (contact or virtual training for a group of staff) 4. Experience with Nob4 5. Awareness training for SME market 6. Remote management and monitoring tools 7. Rim-type tools for managing endpoints remotely
P10	1. KnowBe4 2. Quallace 3. Phish button
P11	1. Mimecast 2.. NoB4 and Trend Micro Phishing insights.3. Siem Technologies: - McAfee ESM - Microsoft Sentinel 4. Antivirus Software: - Symantec Endpoint Protection - Microsoft Defender - Malwarebytes - McAfee Endpoint Protection - Clam AV 5. Network, Email, and Perimeter Protection: - Firewalls (e.g., Cisco, Checkpoint) - Intrusion Prevention Systems (IPS) - Intrusion Detection Systems (IDS) - Mimecast (email security) - Microsoft Exchange Online - Proxy servers (e.g., Blue Coat, Forcepoint, Microsoft) 6. Network Access Control: - Symantec Neck7. Vulnerability Management: - Nessus - Syscat Pro 8. Threat Intelligence: - RSA Archer - Mandiant Intelligence - Cybereason - FireEye Intelligence 9. Recovery: - Backup software (e.g., Dell, Commvault, VMware) 10. Asset Management: - Qualys Global IT Asset Inventory11. Cloud Security: - Zero Trust Networking Architecture (ZTL) - Cisco Umbrella - Check Point – Zscaler 12. Data Security: - Encryption technologies - Masking and anonymisation 13. Identity and Access Management: - Privileged Identity and Access Management (PIAM) - Linear or CyberArk - Conditional access policies 14. Security Awareness: - NoB4 - Trend Micro Phishing Insights
P12	1. Mimecast 2. NoB4 and Trend Micro Phishing insights 3. CASB (Cloud Access Security Broker) 4. Vulnerability management tool 5. Antiviruses 6. Technologies that prohibit file transfer from USB and Bluetooth 7. Email encryption tools 8. Data loss prevention technologies 9. Drive encryption 10. Identity Access Management 11. URL blocking or blacklisting tools 12. Security logs and analysis tools 13. Backup infrastructure for disaster recovery 14. Incident mitigation tools and strategies 15. War rooms for incident response and management
P13	1. EDR solutions (Endpoint Detection and Response) 2. Mimecast servers monitoring 3. Vulnerability scans
P14	The cybersecurity management tools mentioned are1. EDR solutions (Endpoint Detection and Response)2. Mimecast servers monitoring3. Vulnerability scans4. Blue teams (simulated attack exercises)5. Cybersecurity challenges (for normal users)6. Burp - an approximation tool for web applications7. Nmap - a network scanning tool8. Nessus - a vulnerability scanner. Cobalt Strike - a penetration testing tool10. XDR tools (unspecified) - tools used for extended detection and response

Participant Number	Cyber Management Tools
P15	1. NOB4, the phish ER 2. Microsoft Defender 3. Cloudflare 4. Quallace 5. Microsoft Intune
P16	1. Microsoft Defender Sentinel AM 2. Phishing training 3. Hawks hunting (uncertain accuracy) 4. Microsoft Defender (part of Microsoft Defender Sentinel)
P17	1. SIEM (Security Information and Event Management) solution 2. Remote access tools 3. Backup and recovery tools 4. Firewall 5. VPN (Virtual Private Network)
P18	4. Abusive content monitoring tools 5. Copyright Act violation detection tools 6. Criminal activities investigation tools 7. Data breach detection and response tools 8. Tax identity theft detection tools 9. Data exposure detection tools 10. Malicious code activity monitoring tools 11. Ransomware detection and response tools 12. Phishing detection and response tools 13. Physical security validation tools 14. Policy violation detection tools 15. Reconnaissance activity detection tools 16. Unauthorized access detection tools 17. Unpatched vulnerability detection tools
P19	1. Antimalware software 2. Patch management tools (specifically mentioned "Quallace") 3. Incident management systems or logging systems for tracking and recording incidents.
P20	1. Nessus vulnerability scanning 2. Splunk (for event monitoring and log analysis) 3. Data loss prevention (DLP) 4. Cloud solution like Microsoft Azure 5. Exchange (for spam filtering) 6. Vulnerability scanning software 7. Firewalls (for defense in depth) 8. ISO27001 9. NIST (National Institute of Standards and Technology) framework 10. Imaging software (for system recovery) 11. Kali Linux (with built-in cybersecurity tools) 12. Phishing campaigns 13. Bait 14. Cyber awareness program
P21	1. Awareness training document 2. Awareness training videos 3. E-mail security configurations 4. Spam filters or anti-spam measures
P22	I can't disclose this type of information in this interview, but we do have different appliances and tools from different vendors.
P23	1. Mimecast 2. Multi-factor authentication 3. Cybersecurity awareness training
P24	Defender (a tool used as a gatekeeper for incidents and access).
P25	8. Security awareness training tools.
P26	1. EDR solutions 2. McAfee 3. Symantec 4. Windows Defender 5. Antivirus tools 6. Host-based firewall 7. Networking tools 8. Detectors 9. Network intrusion detection system 10. Email security solutions 11. Data DLP (Data Loss Prevention) solutions
P27	1. Cisco Toptan vulnerabilities 2. CVE website
P28	1. DRN (Digital Resilience Network) 2. MDR (Managed Detection and Response) 3. EDR (Endpoint Detection and Response)
P29	1. Phishing campaign for testing awareness and email security. 2. NoB4 platform for sending flyers and newsletters about phishing. 3. Vulnerability management tools. 4. Patch management tools. 5. Cyber Ark. 6. Office 365 tools. 7. Strong password controls. 8. Security awareness training tools.
P30	1. Cyber security awareness 2. Password changing for ex-employee 3. Cyber security capacity 4. Figma (tracks ministry happening due to social engineering) 5. Internal training 6. Developer training 7. Kondo training 8. Phishing training 9. Password management

Source: Researcher's own

Table 4.3 highlights the common themes that emerged from the analysis of these tools, providing valuable insights into the most effective ways to manage cybersecurity-threats. The analysis of the cybersecurity management tools revealed several key themes that emerged from the participants' discussions. One of the most prominent themes was the importance of safeguarding email communications, with a specific tool being mentioned as a key solution in this area, Mimecast. The use of simulated phishing attacks was also highlighted as a crucial step in identifying and mitigating email-based threats. This theme suggests that organisations should prioritise email security to prevent successful attacks. Another theme that emerged was the importance of real-time threat detection and response. The mention of advanced endpoint detection and response solutions and Microsoft Defender suggests that participants value the ability to quickly detect and respond to threats. This theme highlights the need for organisations to have robust monitoring capabilities in place to stay ahead of emerging threats.

The theme of vulnerability assessment and remediation also emerged, indicating the importance of identifying and addressing vulnerabilities in systems and applications. This theme suggests that organisations should prioritise vulnerability scanning as a critical step in maintaining the security and integrity of their infrastructure. Finally, the theme of antivirus software was mentioned, highlighting the ongoing importance of traditional antivirus solutions in protecting against malware threats. This theme suggests that organisations should continue to invest in robust antivirus solutions to complement their more advanced cybersecurity tools.

Table 4.3: Cybersecurity management tools usage common theme

Cybersecurity Management Tools Common Themes	Participants Mentioned
Mimecast	4, 11, 12, 13, 14, 23
Phishing Simulations	1, 5, 9, 10, 14
Vulnerability Scans	13, 20, 29
EDR Solutions	5, 12, 14, 26, 28
Microsoft Defender	11, 16, 26
Antivirus Tools	11, 12, 26

Source: Researcher's own

The COVID-19 pandemic has had a profound effect on the cybersecurity landscape, and professionals in the field have demonstrated the crucial role of social learning in adapting to the evolving threat environment. According to Bandura and Walters' Social Learning Theory (SLT), individuals learn from observing others and their experiences, influencing their behaviour and decision-making (Bandura & Walters, 1977). This theory was applied to analyse the participants' perspectives on the Tools element, highlighting the importance of adopting best practices in cybersecurity. Firstly, participant P6, a cybersecurity consultant, exemplified social learning by embracing the consensus on the value of open-source tools in understanding security incidents, mentioning, that:

> *"I would deploy a lot of open-source tools just so that I can get a better understanding because most organisations only have the basics, antivirus and a firewall."*

The participant further emphasised the importance of these tools in remote work settings, stating that:

> *"The traditional perimeter, represented by the firewall, has diminished in relevance as users operate from home. This necessitates the deployment of open-source tools to collect evidence and analyse logs comprehensively."*

Recent studies have underscored the effectiveness of open-source tools in enhancing incident response capabilities (Liang et al., 2024). Secondly, participant P7, a cybersecurity specialist, also adopted this approach, using tools as a "form of gaining a latch" to search and analyse targets, stating:

> *"We do use tools as a form of gaining a latch. So a latch is the term used to basically just grab on to something that you can then use to search or do a little bit more due diligence on the targets, but we mostly use Boolean. Boolean is basically using the Google language to its advantage."*

The adoption of best practices aligned with recent research by Kour et al. (2023), which demonstrated the significance of using advanced search techniques to pinpoint security vulnerabilities in organisational systems. Thirdly, participant P8, a cyber-defence incident responder, highlighted that:

> *"It was an issue to find the proper tools and resources to distribute the necessary diagnostic tools and implement the proper troubleshooting processes."*

Acknowledging these challenges, the professional drew on his social learning experiences and observations to navigate through incident response obstacles. Recent studies have emphasised the importance of investing in advanced incident response tools to bolster organisational resilience against cyber-threats during remote work scenarios (Karakasilioti, 2024). Participant P13, a head of research development and innovation in cybersecurity, leveraged the SLT by advocating for the use of visualisation tools to help organisations understand their threat landscape, stating that:

> *"We also have a couple of tools that helped visualise the threat landscape for each organisation that we monitor. So we have a couple of vulnerability scans that we do for them when we tell them, like, 'listen up, these are your easier attackable targets'."*

Recent research has supported the use of visualisation tools in cybersecurity risk assessment, underlining their ability to enhance decision-making processes by providing comprehensive insights into complex threat environments (Saeed et al., 2023b). Lastly, participant P16, an experienced information officer and security engineer, emphasised the importance of implementing strong security measures, such as using complex passwords for example stating:

> *"In this meeting room, I could say 'air con chair wall roof,' and that would become my password, and it would be quite secure because an attacker would find it very difficult to brute force that."*

The adoption of best practices aligns with the latest findings in password security research by Rakha (2023), which highlighted the necessity of implementing robust authentication measures to protect against evolving cyber-threats in remote work settings.

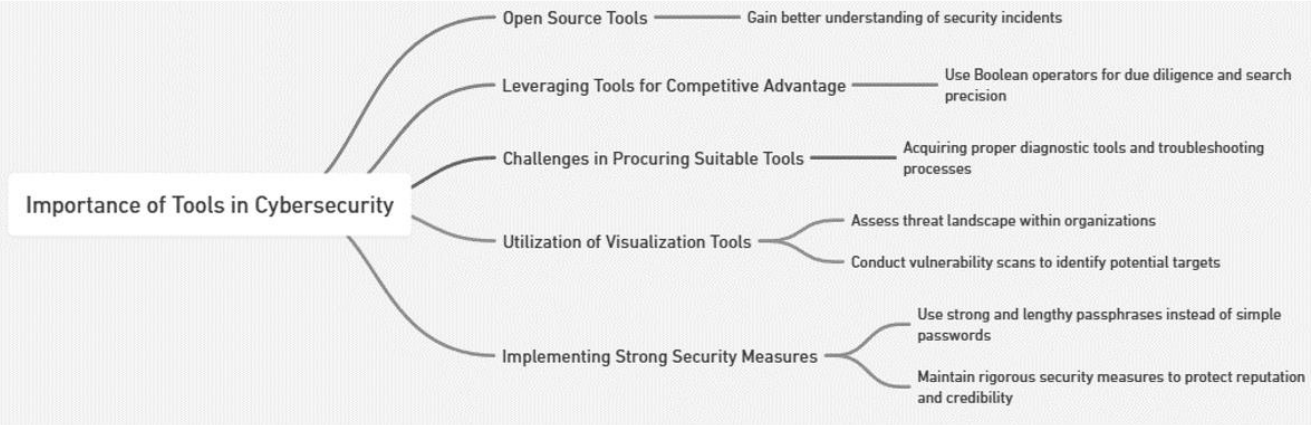

Figure 4.1: Importance of Tools

Source: Researcher's own

4.6 Community element

The Community element underscores the significance of social interaction and collaboration amongst cybersecurity professionals. This fosters an environment for knowledge-sharing, support, and coordination amongst the individuals or groups involved. The community provides an environment for collective learning and problem-solving (Engeström, 2001).

4.6.1 Community common main theme 1: Implementation of policies

Implementing policies in an organisation involves creating, enforcing, and monitoring rules and guidelines to achieve objectives like compliance, risk management, and a safe working environment. The researcher's analysis revealed a common theme in policy implementation.

Thus, organisations prioritised the development and implementation of policies as a critical component of their cybersecurity strategy to mitigate risks, protect sensitive information, and enhance their security posture during the pandemic.

Participant P1, an acting head of information security (IS) governance, highlighted the importance of swift strategy adjustments to address emerging risks in a rapidly evolving environment, emphasising that:

> *"With COVID-19 and the desperate people who wanted to access the policies, you know, they needed immediate access to staff or personnel and I think how we had to change digitally or in terms of technology to set this up, played a big contributing factor in the service that we were able to offer to customers."*

The pandemic has underscored the urgency of technological changes, underlining the need for agile policies to effectively respond to dynamic cybersecurity challenges. Piduru (2022) supported this notion, highlighting the importance of adapting policies to address emerging threats. Participant P3, a cybersecurity consultant, noted:

> *"Because we are so small as a company, we don't really have the need for widespread policies like they do at logical operations".*

According to Sikder and Islam (2023), they emphasised the importance of tailored policy implementation in enhancing cybersecurity resilience for small and medium-sized enterprises

To combat new cybersecurity risks, policies were developed and enforced to secure remote access to systems and mitigate threats like phishing attacks. Participant P7, a cybersecurity specialist, highlighted the importance of proper sub-security policies, stating that:

> *"If they didn't employ proper sub security policies before COVID-19, enforcing it during COVID-19 when your employees are working from home, it's much harder."*

Borkovich and Skovira (2020) supported the concept that COVID-19 pandemic's sudden onset disrupted the development and implementation of remote work policies, leaving many organisations ill-prepared to address insider threats. training and infrastructure (Lang et al. (2023).

Participant P8, a cyber-defence incident responder, emphasised the importance of effective communication and shared responsibility for cybersecurity, stating:

"You had to have policies and people had to stick through to those rules. It was very difficult to start those policies because most of the time people didn't know, they just didn't know whose responsibility was what".

Beyond the policies themselves, successful implementation hinged on communicating policies effectively, establishing shared responsibility for cybersecurity, and providing ongoing education and training to employees. Maathuis and Chockalingam (2022) highlighted the importance of education and communication in strengthening cybersecurity practices within organisations. Participant P9, a cybersecurity director, further emphasised the importance of integrating cybersecurity policies into organisational strategies, mentioning that:

"Policies are connected to the information security management system. So with us and with our clients, as we start off with the security objective within the security strategy, and then the next step is your high-level or your top-tier information security policy, and from your information security policy that focuses on the security objective, then it is rolled out into your second-tier policies - that is quite a range".

The integration of cybersecurity policies into organisational strategies was crucial, as they significantly supported an organisation's mission and vision. Al-Hawamleh (2024b) accentuated the importance of aligning cybersecurity policies with organisational objectives for enhanced effectiveness.

4.6.2 Community common main theme 2: Cultivating a cybersecurity-aware culture and environment

The concept of cultivating a cybersecurity-aware culture involves promoting behaviours, attitudes, and practices that prioritise and enhance cybersecurity within an organisation. Participants emphasised the significance of fostering a culture of cybersecurity awareness and education, creating proactive and resilient cybersecurity measures in response to the COVID-19 pandemic's challenges.

Participant P1, from an organisation with over 50 people, emphasised the need to expand cybersecurity understanding beyond work laptops, stating that:

"Cybersecurity is bigger than just your computer at work... It's your digital footprint."

This aligns with Mughal (2020), who stressed the importance of educating employees about the risks associated with their digital activities. Participant P6, from an organisation of 10 people, highlighted that:

"Curiosity was the biggest thing when we had engagements with staff to ask why you clicked."

This approach is supported by research on interactive training methods, such as Mungo (2023), who advocated for interactive training methods to enhance cybersecurity awareness and behaviour.

Participant P7, working with 10 people, placed more emphasis on advising staff and trusting their maturity, stating that:

"We pretty much advise on what to do - We hope our staff are more adults than anything else".

This approach is supported by research on trust and maturity, which suggests that individuals who are trusted and empowered to make decisions are more likely to take ownership of their work and adopt secure behaviours (Alshaikh & Adamson, 2021).

Participants highlighted the critical role of staff training within organisations. Participant P17, working in an organisation with over 500 employees, stressed that:

"If your staff is not trained enough, then you're just wasting your time because it is a matter of time till you get breached".

This aligns with the insights of Bada and Nurse (2019), who highlighted how insufficient training leaves organisations susceptible to breaches. Participants emphasised the importance of raising awareness in preventing and mitigating social engineering attacks. Participant P30, working in an organisation of over 200 people, highlighted that: *"The first thing is to make people aware"*. This aligns with Hove (2020), who stressed the significance of boosting employees' awareness of social engineering tactics to thwart successful attacks.

Participants in the study shared various strategies for fostering a culture of cybersecurity awareness within their organisations. These strategies aimed to educate employees, promote collaboration, and encourage knowledge-sharing. One approach was to engage in community efforts and discussions to raise awareness about cybersecurity topics. Participant P2, working in an organisation with over 10,000 people, suggested that:

"What we do is engage in discussions at conferences, write blog posts, and join community efforts to raise awareness about various topics. Recently, we have also formed partnerships with the blue team, which is a group of security professionals who

provide solutions to protect against cyber-threats. This collaboration allows us to offer our clients exclusive deals, such as an add-on for their browsers that helps detect and prevent phishing attacks. So, yes, we are actively involved in these initiatives."

Another approach was to educate employees through personal stories and experiences. Participant P3, working in an organisation with over 50 employees, shared that:

"Just educating other people, it sounds like a blog about what they do and then from there, hopefully, people will read it, try to like, create their own security measures, you know."

In addition to these approaches, participant P4 noted that:

"Monthly articles - basically just get steps of what's been happening within the cyberspace and then share it with the employees as well."

Personalised communication was also highlighted as a key strategy for user education. Participant P8 emphasised that:

"It's important to communicate with users on an individual level, whether it's through email or WhatsApp groups, personalised messages and customised information make people feel more comfortable and approachable."

Participant P9 further stressed:

"We actually have a programmer's source. So we provide newsletters, writings, and blogs to our clients."

However, participant P28 noted a different trend, where organisations often hoard knowledge, hindering cybersecurity efforts, stating that:

"When it comes to defenders, most companies tend to keep knowledge to themselves because it becomes their intellectual property. So if I share with another company, we are essentially sharing the money-making strategies. Until companies on the defending side break that, we will not be able to start catching up on these attackers."

This sentiment is supported by Alhogail (2021), who found that collaboration and information-sharing amongst cybersecurity professionals have a positive impact. Thus, it is crucial to be able to create a knowledge sharing environment.

4.7 Division of labour element

The Division of Labour element involves the allocation of tasks and responsibilities amongst individuals or groups within the activity system. It acknowledges the need for different roles and expertise to achieve the objectives of the activity, ensuring efficient resource utilisation and promoting specialisation in the system.

4.7.1 Division of labour common main theme 1: Comprehensive security controls, team processes and addressing skills scarcity

Thematic analysis reveals a shared concern for comprehensive security controls and skills scarcity, indicating common strategies amongst participants in addressing critical cybersecurity management aspects. Participants emphasised the significance of implementing robust security measures to combat cyber-threats and acknowledged the challenge of locating skilled professionals in the cybersecurity field.

Participant P9, a cybersecurity expert with a PhD in Computer Security from the University of South Africa, emphasised the need for *"Proper controls in-depth kind of approach"* to mitigate potential attacks. This concept aligns with the defence-in-depth strategy, which involves deploying multiple layers of defences to create overlapping barriers against potential attackers (Ning & Jiang, 2022). However, participant P9 highlighted the challenge of cybersecurity skills scarcity, noting that:

> *"there is a big or massive lack of skills"* and *"if you look at that, you say, oh, you know what, then there was a big issue."*

This scarcity is linked to the cybersecurity skills gap caused by evolving threats and inadequate education and training programmes (Jordan, 2022).

Participant P11, a cybersecurity expert with a Master of Technology in Computer and Information Systems Security and Information Assurance from the Cape Peninsula University of Technology, further emphasised the importance of continuity in cybersecurity practices during the pandemic, stating:

> *"The COVID-19 threats wouldn't follow a different process, right? So the process we followed prior to COVID-19 would apply as basically, you know, what addressing risk in dealing with vulnerabilities and remediating things."*

This approach is reflected in the comprehensive protection approach by combining risk management disciplines (Stine et al., 2020). This method helps organisations address cybersecurity risks during disruptions, ensuring critical system and data continuity.

Participant P13, a cybersecurity expert with a Master of Science in Computer Science from the University of Pretoria, highlighted the importance of proactive measures in identifying and fixing system vulnerabilities, mentioning, that:

> *"We have a couple of vulnerability scans that we do for them when we tell them, like, listen up, these are your easier attackable targets, and we run blue teams of them, and what we have also now started doing for all the normal users is having cybersecurity challenges where we create cyber challenges for the normal person to try and see if they can hack into a system."*

This approach aligns with Rantalaiho (2024), who emphasised the importance of vulnerability scans, continuous monitoring, and cybersecurity challenges in identifying and fixing system vulnerabilities.

4.7.2 Division of labour common main theme 2: Efficient task allocation and responsibility-sharing

During the thematic analysis, the common theme of efficient task allocation and responsibility-sharing emerged as participants discussed their experiences with dividing labour and resources effectively to achieve organisational goals. This theme was identified through the shared recognition of the importance of clear delegation of tasks, roles, and responsibilities to enhance productivity and collaboration within their teams.

Participant P5, a cybersecurity and technology risk consultant with 10 years' experience, noted that:

> *"We had to now move all our critical systems into a managed SOC team. Where this 24-hour monitoring and response is also adopted, we have adopted EDRs [Endpoint Detection and Response] for device detection and response."*

This approach is in line with Erdıvan's (2024) recommendations for effective cybersecurity management, which stressed the necessity of maintaining dedicated SOC teams and utilising advanced technologies like EDRs for effective cybersecurity operations. By assigning specialised roles within the SOC team, organisations ensured that individuals possessed the

requisite skills and knowledge to carry out specific tasks, including continuous monitoring, incident response, and threat hunting.

The importance of specialisation in cybersecurity operations was also highlighted. Participant P3, a cybersecurity consultant with five years' experience, emphasised:

> *"So if there are any incidents, then a few of the team will join. They call it the war room. When there's something really intense happening and we need to stop someone, you know, like immediately. So we'd all jump in at the same time."*

This aligns with Nyre-Yu's (2019) research on the benefits of division of labour and specialisation in improving productivity.

Effective coordination and communication were stressed as critical components of cybersecurity operations. Participant P15, a cybersecurity engineer with five years' experience, highlighted the importance of clear and concise communication during cybersecurity incidents, stating that:

> *"The responsibilities split, so cybersecurity is not just an information security responsibility - What we would do as information security would be to talk to you directly and say, 'Listen, this is what happened because we don't know. What we don't want to do is cause panic from your side."*

This viewpoint resonates with literature advocating for a holistic approach to cybersecurity, stressing the need for cooperation and shared responsibilities across teams and departments (Jha & Jha, 2023).

The importance of access control was also emphasised by participant P30. This cybersecurity software engineer in Cape Town, with seven years' experience, brought up the importance of revoking access for departed employees, stating that:

> *"In my observation of various companies, I have witnessed the process of revoking access to certain services for employees who have left many years ago, while still claiming to be actively employed, and it became apparent that there were only five visible windows due to remote desktop connections, whereas the actual processing was questionable, leading to concerns about the repercussions for those who resign or are terminated, including managers, as well as the circumstances surrounding employees who have left their jobs."*

This highlights the Principle of Least Privilege (Saltzer & Schroeder, 1975), which advocates for granting minimal access required for job functions (Bernal, 2009). In conclusion, revoking access rights to former employees is a critical step in ensuring the security and integrity of a company's systems and data, and should be a top priority for any organisation that values its sensitive information.

4.8 Rules element

During the COVID-19 pandemic, cybersecurity professionals adhered to rules governed by the Protection of Personal Information (POPI) Act, number 4 of 2013, hereafter referred to as the POPI Act (South Africa, 2013). Compliance with the POPI Act ensures the lawful and secure handling of personal data, safeguarding it from unauthorised access or misuse.

4.8.1 Rules common main theme 3: Relevance of industry frameworks and standards

Participants highlighted the significance of complying with industry frameworks and standards like the US National Institute of Standards and Technology (NIST), ISO, and the US Center for Internet Security (CIS) to showcase an organisation's commitment to cybersecurity best practices. Adhering to these guidelines fosters efficient incident management, demonstrating a proactive stance towards cybersecurity risk mitigation.

The Institutional Theory, as outlined by Burdon and Sorour (2020), emphasises the importance of industry frameworks and standards in cybersecurity. These guidelines are influenced by external pressures from stakeholders like customers, regulators, and peers, demonstrating organisations' commitment to cybersecurity and mitigating risks. Participant P20, a cybersecurity manager, and participant P23, a senior cybersecurity consultant, both emphasised the importance of following industry frameworks. Participant P20 stated that:

> "*Every company should follow a cybersecurity framework such like NIST, ISO, and CIS",*

and participant P23 stating that:

> "*All organisations will have an organisational IT security policy - NIST cyber security framework being the more popular ones".*

These frameworks are not only recognised as best practices but also serve as institutional pressures for organisations in the cybersecurity sector to establish and uphold effective cybersecurity measures (Ogbanufe et al., 2021). By adhering to these standards, organisations

can signal their legitimacy and credibility to stakeholders who prioritise robust cybersecurity practices. Participant P26, an IT security analyst with over seven years' IT and cybersecurity experience, noted that:

> *"We do have enough standards - ISO 7001, the standard we are compliant to and also COBIT, yes, that is for governance and your ITIL for incident management."*

The existence of standards that were adhered to in the past, such as International Organization for Standardization (ISO) 27001 for compliance and Control Objectives for Information and Related Technology (COBIT) for governance, along with utilising Information Technology Infrastructure Library (ITIL) for incident management. Complying with these standards not only assists organisations in managing and responding to security incidents more effectively but also aligns them with the expectations of their institutional environment (D'Arcy & Basoglu, 2022). This emphasis on following established standards is in line with recommendations from cybersecurity scholars (Al-Hawamleh, 2024a) advocating for implementing industry best practices to bolster cybersecurity defence mechanisms.

The discussion touched on the importance of legislation in combatting cybercrime. Participant P11, a security solutions architect with considerable technology and cybersecurity expertise, pointed out that:

> *"The lack of legislation in African countries made them more appealing targets for cybercriminals."*

This observation resonates with existing literature, further underscoring the significance of robust cybersecurity strategies in these regions (Kritzinger, 2020). This emphasises the need for comprehensive cybersecurity strategies, legislation, adequate resource allocation, and training to enhance cyber-defences in developing countries. Institutional Theory explains the necessity for comprehensive cybersecurity strategies and legislation in developing countries, which often lack the institutional structures and regulations essential for robust cybersecurity practices, making them more vulnerable to cyber-threats (Singh & Alshammari, 2020).

Participant P9, a director with over 21 years' IT and cybersecurity experience in the retail / fashion industry also noted the absence of a nationwide cybersecurity strategy in the past from a government perspective. They highlighted that:

> *"From a government perspective, we still don't have a cybersecurity strategy nationwide - Do we? You know, POPI is the only sort of regulation in terms of compliance that is around."*

This observation is in line with critiques from cybersecurity experts (Malatji et al., 2020) who have pointed out the lack of comprehensive national cybersecurity strategies in various countries, such as SA. Participant P18, a senior IT security engineer with over six years' IT and cybersecurity experience in the technology / software industry, noted that:

> *"We didn't have regulations in place until recently with POPIA, but there were still many attacks happening as SA was listed amongst the top ten countries for cyber-attacks."*

This indicates that despite the regulatory gap, a significant number of cyber-attacks have been observed in the SA, thus Johns (2020) highlighted the global prevalence of cyber-attacks and the urgent need for robust cybersecurity regulations in SA to address and mitigate this growing threat. Participant P20, an information security analyst with more than four years' IT experience and over three years' cybersecurity experience, highlighted:

> *"Funding for cybersecurity was limited -However, new legislations like the cybercrimes bill and POPIA were driving the awareness of cybersecurity in the country."*

This finding aligns with research by cybersecurity experts Sekgololo (2020), emphasising the importance of legislative measures in driving cybersecurity awareness and resilience. To further confirm previous findings, participant P24, an IT governance, risk and compliance manager with over 13 years' IT experience and more than two years' cybersecurity experience, expressed that, *"What makes us vulnerable as a country is the lack of laws that we have around it."* Their expertise in IT governance and compliance emphasises the crucial role of regulatory frameworks in protecting against cyber-threats. This perspective can be further supported by the notion that implementing legal policies and laws cannot fully address cybersecurity issues, but consulting with technologically advanced security experts is crucial to fortify the existing legislative framework and prioritise international legal protections and guidelines, especially in the rapidly digitising African continent (Olofinbiyi, 2022). The participant's assertion was corroborated by participant P20, a cybersecurity manager, who mentioned that, *"We had a lower level of cyber maturity in SA compared to first-world countries."* This observation aligns

with the findings of previous research, which delineated the challenges encountered by developing countries in establishing resilient cybersecurity measures (Singh & Alshammari, 2020). Kritzinger (2020) outlined challenges faced by developing countries in establishing resilient cybersecurity measures. Limited resources, skills, and regulatory frameworks hinder progress in achieving cyber-maturity in these countries. Thus, the lower cyber-maturity in SA emphasises the need for improvement and adoption of best practices to combat escalating cyber-threats in the region.

4.9 Object element

The Object aligns with the activities of a cybersecurity management system by focusing on the actions employed by cybersecurity professionals. Key activities in a cybersecurity management system involve conducting risk assessments, deploying secure remote access solutions, enhancing employee awareness and training, and implementing incident response plans.

4.9.1 Object common main theme 1: Phishing simulation and awareness training

In the realm of cybersecurity, the strategic implementation of regular phishing simulations and awareness training programmes emerged as a pivotal action against potential threats. This multifaceted approach involves not only testing the resilience of organisational defences but empowering employees with the knowledge and skills to recognise and respond to phishing attempts effectively.

4.9.1.1 Sub-theme: Phishing simulation techniques

Past research has emphasised the importance of aligning simulated phishing attacks with established industry guidelines and best practices. Participant P1, a vulnerability assessment expert, underscored the significance of these simulations by stating:

> *"These simulations were designed to mimic actual phishing attempts and were internally benchmarked against real-life scenarios."*

This approach sheds light on the proactive strategies that organisations can employ to bolster employees' awareness and response to phishing-threats. This echoes the advice of cybersecurity experts who advocate for immersive hands-on training to empower employees in identifying and thwarting phishing attacks (Roepke et al., 2020).

Participant P10, a Certified Information Systems Security Professional, highlighted the importance of phishing simulations in identifying and mitigating phishing-threats. They explained:

> *"Things like phishing simulations where I would send a person an email from a spoofed email address and check if they fall for the text and look out for things like misspellings, incorrect formatting, or the use of critical naming. This way, you can identify a phishing email and have a 'phish' button to report it."*

This participant's specialised knowledge lends credence to the effectiveness of phishing simulation techniques in pinpointing and mitigating phishing-threats within organisational settings. This underscores the importance of integrating industry expertise into cybersecurity training initiatives to ensure their efficacy (Hakimi et al., 2024).

Participant P12, with a BCom in Management Information Systems from the University of Western Cape, shared a notable experience that:

> *"We got a lot of phishing reports from a lot of staff, and this was increased in volume. A lot of staff were reporting that they were receiving these emails, whether it was from a Mastercard or from some kind of online consumer company."*

This corroborates the prevailing notion that active phishing simulation exercises can foster a vigilant organisational culture in the face of evolving cybersecurity-threats.

4.9.1.2 Sub-theme: Cybersecurity Training and assessment methods

An examination of past training and assessment methods revealed a need for harmonisation with adapting to remote work, specifically to enhance the effectiveness of the cybersecurity-aware culture and environment under the Community element, building upon the actionable steps previously discussed. Participant P5, a cybersecurity expert, emphasised the importance of addressing the "*People aspects of cybersecurity*" by introducing cybersecurity awareness tools and interactive training platforms. According to participant P5:

> *"The people aspects of cybersecurity were the one that we needed to deal with so we brought in cybersecurity awareness tools like KnowBe4 to assist a user when training simulations, phishing simulations, and the likes for benchmarking and targeted training."*

This approach aligns with the Social Learning Theory (SLT), which suggests that individuals learn by observing others and imitating their behaviour (Bandura, 1977). Interactive training platforms provide opportunities for employees to observe and learn from simulated phishing-threats, helping to educate them about potential cybersecurity risks (Alhashmi et al., 2021). By utilising benchmarking and targeted training, organisations can identify knowledge gaps and tailor their training programmes accordingly, aligning with the principles of SLT.

Participant P6, working in the technology and security industry, highlighted the importance of *"Changing the security paradigm by emphasising hygiene."* This is achieved through the "Triple Ts" approach, which includes testing, training, and targeted exercises. According to P6's organisation:

> *"The Triple Ts approach, which includes testing and training employees. After training, we assess their knowledge through quizzes. Additionally, we conduct purple teaming exercises to evaluate their response to real-world scenarios."*

This approach reflects the principles of Experiential Learning Theory (ELT) and Action Learning Theory (ALT), which emphasise the importance of hands-on experience and applying knowledge in real-world scenarios to drive learning and growth (Kolb, 1984; Angafor et al., 2020).

Participant P13, who works in the technology and security industry, took a gamified approach to cybersecurity training:

> *"We have a couple of awareness programs, and what we have also now started doing for all the normal users is having cyber challenges where we create cyber challenges for the normal person to try and see if they can hack into a system. Just to show them how easy some of these attacks actually are."*

This approach aligns with the Cognitive Load Theory (CLT), which suggests that individuals have a limited capacity for processing information, and effective learning occurs when information is presented in a manner that optimises cognitive load (Kolb, 1984). Thus, by engaging users in gamified cybersecurity challenges, organisations can increase motivation and attention, making the learning process more effective (Wu et al., 2021).

In addition to these approaches, Participant P28 from the financial services industry highlighted the importance of encouraging employees to actively participate in cybersecurity efforts:

> *"Some companies have now deployed technologies where users can report some of these phishing attacks, or as and when they come in, they report anything they feel is suspicious. I know some of our clients reward employees for reporting such instances."*

This approach aligns with existing literature that emphasises encouraging employees to actively participate in cybersecurity efforts (Mitcham, 2024). The literature has noted the importance of organisations implementing reporting systems to facilitate the submission of incident reports. By enabling employees to easily report phishing attacks, organisations promote a stronger cybersecurity culture within their workforce. The literature has examined the effectiveness of rewarding employees for reporting instances of phishing. This practice demonstrates an organisation's commitment to building a positive cybersecurity culture and incentivises vigilant behaviour. Previous studies have shown that implementing a reward system for reporting incidents can significantly improve the overall reporting rate (Slonka et al., 2023).

The COVID-19 pandemic led to unprecedented challenges for organisations, including maintaining business continuity and ensuring the security of employees and data. As companies transitioned to remote work, they had to quickly adapt to new technologies, workflows, and cybersecurity-threats. In this context, cybersecurity training and awareness became essential for organisations to educate and equip employees to handle the unique challenges of working from home. Participant P19 insights into the importance of adapting cybersecurity training and awareness strategies to meet the changing needs of remote work, mentioning that,

> *"Before COVID started...there were a lot of scams going around the Internet asking people to click here and here to learn more about COVID-19...So we quickly had to change our perspective and be more secure."*

This aligns with the literature on the importance of contextually relevant and tailored training programmes that address specific job roles and environments (Fagbule, 2023). Adapting training content to the remote work context ensures that employees receive targeted guidance and support to navigate the unique cybersecurity challenges associated with working from home.

In terms of cybersecurity awareness campaigns, Participants P19 and P20, senior technical information and cybersecurity services specialist, and information security analyst respectively, discussed the incorporation of COVID-19 themes into their training content. By leveraging current events and issues, organisations can create relatable training content that

increases employees' understanding of the specific risks and challenges associated with COVID-19-related scams and phishing campaigns. This aligns with the theory of situated learning (Lave & Wenger, 1991). The study also highlighted the importance of weighing costs and benefits when making decisions about remote work shifts (Homans, 1958).

Participant P20 emphasised the importance of using current events and topics to exploit human vulnerabilities, stating:

> *"When COVID started and people were working from home, then we had to oppose and make sure that we sent a lot of content...related to how they work now or how they were currently."*

This aligns with the concept of SIT (Cialdini, 1993), which suggests that people are more likely to respond to requests that are consistent with their existing attitudes and behaviours. Participant P20 highlighted the effectiveness of using COVID-19 information in phishing campaigns:

> *"We have used COVID-19 information such as vaccine...in some of the phishing campaigns...so yes, those were two years basically."*

This demonstrates the importance of using current events and topics to simulate real-world scenarios and exploit human vulnerabilities.

Regular training activities played a crucial role in keeping employees aware and updated on cybersecurity-threats. Participant P4, a deputy director of protection services, emphasised the importance of consistent engagement:

> *"On a monthly basis, we would at least send out through activities…which were compulsory... Focusing on a topic of a week."*

This approach aligns with the literature on the effectiveness of regular training in keeping employees aware of cybersecurity-threats (Hijji & Alam, 2022).

Participant P15, a cybersecurity engineer, highlighted the importance of concise training sessions:

> *"There's training that you could push out, like 5-minute videos and then like a quick test... To ensure that the staff members are aware of what the phishing attack may look like."*

This approach aligns with the theory of microlearning, which suggests that short and focused training sessions are more effective in capturing and retaining employees' attention (Loh-Joey, 2021).

4.9.2 Object common main theme 2: Multi-factor authentication implementation

The common theme of the relevance of industry frameworks and standards in the implementation of MFA was identified through the analysis of the participants' experiences that highlighted the importance of aligning security measures with established guidelines and regulations to enhance overall cybersecurity resilience. During the discussion on MFA implementation, participants highlighted the importance of persuasive communication to gain executive and managerial support. Participant P10, with over 17 years' IT experience, emphasised that:

> *"We had to persuade the CEO, persuade the managers, and they had to recognise that it was a vital thing to prevent the threats. It's actually vital that you use multi-factor authentication because - if credentials are stolen, it could lead to things like business email compromise that could lead to bigger disasters"* and added, "*Technical implications became a massive cost implication because many organisations didn't have the capability for multi-factor authentication."*.

This aligns with existing literature on MFA adoption challenges, where perceived behavioural control, as per the TPB (Ajzen, 1991), influences employees' intentions to adopt MFA based on the technical complexities. Participant P10's statement highlights the need for effective change management strategies in cybersecurity measures adoption, aligning with Omoyiola and Mckeeby's (2023) findings. Persuasive communication can influence subjective norms, impacting employees' intentions to adopt MFA positively.

Participant P18, with six years' experience in IT, underscored the importance of organisational policies in driving changes and technology adoption:

> *"Look, we are within our organisation's IT policy, and there is also subsequent, information security policy and ICTS policy to drive changes and also, you know, if the policy is in place, then you can measure against that in your effectiveness as well. If there's something that happened, you can refer back to the policy, like for example, our motivation to enable MFA."*

Literature emphasises aligned organisational policies to drive security practices and technology adoption (Kunduru et al., 2023). External factors like organisational policies influence perceived behavioural control over MFA usage and intentions to adopt it.

Participant P17, a cybersecurity specialist, acknowledged that:

> *"The majority of organisations based off of what I've seen have implemented - MFA, single-sign-on, but that can also be kind of a risk."*

This statement is consistent with literature on MFA risks and security challenges like reliance on a single device and social engineering attacks (Tolbert, 2021). External barriers like maintaining secure single-sign-on capabilities affect perceived behavioural control over MFA usage and intentions to adopt it. Participant P23, with two years' IT experience, highlighted:

> *"So you want to protect your identity? Simple things like stronger passwords. Multi-factor authentication Those are actually vital. They are the basics and the vital elements to protecting the identity because that's what the attacker targets. He wants to get your information, your login details, and so forth."*

Individual attitudes towards multi-factor authentication (MFA) and strong passwords play a crucial role in determining one's intentions to adopt and utilise these measures. This aligns with the existing body of research, which consistently highlights the importance of MFA and strong passwords for effective identity protection (Das et al., 2020).

Participant P11, with over 13 years' IT experience, warned of cybercriminals bypassing security measures. The participant noted that:

> *"There's definitely an increase in phishing - a lot of companies are implementing multi-factor authentication by default. So needless to say, you know cyber-criminals are looking at ways to get around that."*

This statement underscores the ongoing challenge of data protection (Belmabrouk, 2023). Participant P17 cautioned that:

> *"So the way that it changed now is that obviously people couldn't go into work and everything was done on a device that would need to be. Managed, or secured remotely. So that means that the networks or the Internet, the Wi-Fi that we connect to would be, external devices. That are connecting to company resources like your home Wi-Fi, your home Wi-Fi is compromised, there has to be additional security controls that are in*

place like we had like VPN multi-factor authentication. So majority of organisations based on what I've seen have implemented, obviously a work from home policy and the first thing is always VPN access and multi-factor authentication. And then obviously it also single sign on. So single-sign-on is kind of a different thing because we may have single-sign-on. We have to make sure that it integrates with all other systems just to make it easier for users. But that can also be kind of a risk, so in the context of COVID, everywhere phishing attempts have obviously been increasing and the larger the phishing pool, the more likely your chances are actually getting credentials and then organisations network and obviously be compromised".

This can be explained further that COVID-19 pandemic has underscored the necessity of crafting and implementing flexible security measures that can adapt to the rapidly changing threat landscape. As security fatigue becomes a growing concern, it is essential to recognise its potential consequences, including decreased employee attention and increased susceptibility to phishing attacks, as noted by Nobles (2022). Consequently, to mitigate these risks, organisations must adopt a forward-thinking approach to security, incorporating advanced threat detection and response capabilities. This may involve employing machine learning and artificial intelligence to analyse threat patterns and identify vulnerabilities, as well as regularly providing security awareness training and phishing simulations to educate employees on the latest tactics and techniques used by attackers. By taking these steps, organisations can significantly reduce the likelihood of security breaches and ensure the continued confidentiality, integrity, and availability of their sensitive data.

4.9.3 Object common main theme 3: Remote work adaptation

The COVID-19 pandemic has brought about a significant shift to remote work, presenting new challenges and vulnerabilities in the realm of cybersecurity. Participants in the study shared their experiences and insights, highlighting the importance of understanding the unique challenges and risks associated with remote work.

The transition to remote work environments has been a major factor in the increased risk of cyber-threats. As participant P11, a security solutions architect in the energy / petroleum industry, and participant P29, a cybersecurity manager working in professional services / accounting, noted:

"Organisations couldn't manage their networks effectively because of the whole work from home, which was the head office network".

This sentiment is consistent with existing research on one of the vulnerabilities introduced by remote work (Bispham et al., 2021). Building on recent studies, the shift to remote work has amplified the threat of cyber-attacks, particularly phishing campaigns, due to the challenges organisations face in maintaining robust network management and security protocols (Jimmy, 2024).

The shift to remote work was a notable phenomenon during the pandemic, as participant P11 acknowledged:

> *"So with COVID-19, I'd say the most notable thing was a shift from people working from the office to people working from home."*

This external pressure led to a collective change in behaviour. For participant P11, one of the biggest challenges was *"getting hold of users, due to the nature of everything."* Organisations should have promoted collective responsibility and open communication about risks, influencing individuals to be more cautious. The Technology Acceptance Model (TAM) explains individuals' behaviour in remote work and cybersecurity based on their perceived usefulness and ease of use of cybersecurity measures. Organisations could have encouraged the adoption of user-friendly cybersecurity tools and other cybersecurity measures by highlighting their usefulness and simplicity (Sala & Martiri, 2023). Participant P1, an acting head of IS governance working in the technology / software sector, noted that:

> *"Previously, our staff were obviously based at the offices, when COVID hit, we had to quickly adapt and change the way we have enabled everyone at our organisation. To work remotely, so we gave everyone remote laptops,"*

aligning with research on rapid transitions (Olawale et al., 2024). Some participants believed that the shift to remote work was driven by cost considerations. Participant P9, a director in the retail / fashion industry, mentioned that:

> *"Many of the organisations shifted online, because they had no choice, I believe it was a cost issue because it was required,"*

echoed by participant P12, an IT delivery manager in cybersecurity working in the retail / food and beverage industry, acknowledged that:

> *"Because we were remote workers, everything changed. The environment changed, the way that we looked at security, changed. But it was a bit of a late realisation".*

This further highlighted the need for swift security adaptations (Arunprasad et al., 2022).

In contrast, other participants noted that their organisations were already prepared for remote work, reflecting crisis management best practices (Hatton & Brown, 2021). Participant P8, a cyber-defence incident responder, observed that:

> *"COVID hasn't really impacted it that much. Since everything was already done remotely",*

supporting the importance of pre-existing flexible infrastructures and policies (Caldeira et al., 2023). This observation underscores the significance of proactive measures in maintaining cybersecurity resilience during unexpected events. Participant P22, a senior specialist in IT security, observed that *"we were already geared up for COVID-19 remote work,"* which aligns with discussions on balancing speed and security during remote work transitions (Kaushik & Guleria, 2020). In terms of proactive measures, participant P23, a senior cybersecurity consultant, suggested:

> *"COVID-19 pandemic had a minimal impact on our ways of working as our organisation provided laptops to its employees, making the transition to working from home seamless. However, additional costs were incurred to provide internet connectivity for those who didn't have it at home. Our infrastructure already allowed for flexibility, with the only adjustment being the need to ensure internet access for logging onto our network and systems via VPN."*

In addition, participant P14, a cloud penetration tester, reported that:

> *"It didn't impact my work in any way...it wasn't a train smash at all."*

Despite the potential severity of the situation, their experience was relatively uneventful and did not cause any disruptions or challenges. The collective expertise of participants P8 and P23 who worked in technology security in education and healthcare respectively, and participants P22 and P14, who both worked in the financial sector, underscores the significance of their contributions to the discussion on cybersecurity best practices. As they are already familiar with the vulnerabilities inherent in their respective industries, they bring a unique perspective to the table. Their experiences in high-risk environments have likely prepared them to anticipate and address potential threats.

Participant P10, a cybersecurity executive consultant with extensive IT and cybersecurity experience, highlighted the importance of adequate resources in enabling remote functionality:

> *"If you look at the impact generally across all organisations, the first impact was the massive mobilisation of resources...but it takes almost three years for some organisations to get to a point where they can actually be functional directly from home."*

This underscores the time and effort required for a successful transition. This aligns with research by Carvalhaes et al. (2020), who emphasise the importance of adaptive infrastructure in maintaining business continuity during disruptive events. Participant P10's insight highlights the critical role of adequate resources in enabling remote functionality and emphasises the need for organisations to invest in robust infrastructure to support remote work practices efficiently. The observation emphasises the critical role of adaptive infrastructure in maintaining business continuity during disruptive events (Dewi, 2024). Participant P10's insight highlights the need for organisations to invest in robust infrastructure to support remote work practices efficiently.

Participant P11, a security solutions architect, emphasised:

> *"So with COVID-19, I'd say the most notable thing was a shift from people working from the office to people working from home,"* adding that, "*getting hold of users was probably the biggest challenge."*

This perspective aligns with the findings of Malik and Garg (2020), who stress the significance of user engagement and communication in enhancing organisational resilience. Effective communication with users is essential in ensuring smooth transitions to remote work and maintaining productivity in remote work environments.

Participant P25, an IT governance and security analyst, shared insights on the technological challenges faced in implementing a work-from-home scenario. They noted that:

> *"Technology wise, we're not fully prepared for their whole work from home scenario. So we had to make sure that we came up with a strategy very quickly. In order to have the correct technologies, that meets our security requirements."*

They also mentioned issues with licensing and bandwidth:

> *"Yes so these technologies are license-based, so we had issues of not having enough licenses. So, meaning that whoever needs to be connected, we shouldn't just be giving*

people connection. We have to make sure that we have enough licenses and we also had issues on the bandwidth side. On the bandwidth side, we were not prepared.".

However, their experience underscores the need for organisations to develop strategies and adopt technologies that meet security standards and enable remote access efficiently. This aligns with the concept of digital resilience, emphasising the importance of technological readiness in enhancing organisational resilience during crises (Forliano et al., 2023).

4.9.4 Object common main theme 4: Incident response plan adaptation

Incident response is a reactive measure aimed at responding to and containing security incidents after they have occurred (Shinde & Kulkarni, 2021). The adaptation of incident response plans as a common theme was derived from participants revising and updating their response strategies and protocols to address the evolving nature of cyber-threats during the COVID-19 pandemic, ensuring a more robust and effective approach to managing and mitigating cybersecurity incidents.

According to participant P17, working in a company with over 500 employees in the telecommunications industry:

> *"User awareness and the implementation of security tools like firewalls and VPNs, outlined in a security baseline configuration document, are crucial in incident response."*

Mwangi (2024) notes that user education and the use of security tools like firewalls and virtual private networks (VPNs) are essential in mitigating cyber-threats. This suggests that organisations should not only focus on technological measures but also educate their users to recognise and respond to potential threats.

Participant P19, working in a company with over 5,000 people in the education industry, emphasised:

> *"Organisations employ playbooks as step-by-step guides for dealing with various incidents, recognising the diversity of threats such as phishing, malware, and network intrusions."*

This aligns with existing literature on the importance of incident response playbooks (Van der Kleij et al., 2022). The participants' experience in both IT and cybersecurity adds credibility to their insights on developing and implementing incident response playbooks.

Participant P27, working in a company with approximately 200 employees in the technology and security industry, highlighted:

> *"Understanding the target, the nature of the attack, and the data at risk is pivotal. Threat playbooks, designed for scenarios like DDOS attacks and ransomware, incorporate reconnaissance as a crucial step in defence."*

This aligns with existing literature on the importance of understanding the nature of the attack and targeted data for effective incident response (Schlette et al., 2021). Participant P28, working in financial services, emphasised the importance of prioritising system backups before attacks:

> *"Prior to attacks, organisations should prioritise system backups to facilitate data recovery in the event of data loss."*

This aligns with literature on data backup and recovery measures in incident response planning (Safitra et al., 2023). Participant P28's managerial role suggests their experience and expertise in overseeing incident response processes, adding reliability to their insights.

4.9.5 Object common main theme 5: Prioritisation of patching

In contrast to incident response, patching is a proactive measure aimed at preventing security incidents (Jones, 2022). The theme of prioritising patching efforts was shaped by participants' recognition of the critical need to promptly apply security patches and updates to mitigate vulnerabilities and strengthen their cybersecurity posture, especially as the frequency and severity of attacks increased during the pandemic. Einler Larsson and Qollakaj (2023) highlight the increased risks associated with remote work, as it introduces more potential entry points for attackers.

Participant P10, a cybersecurity executive consultant, emphasised:

> *"Our organisation looked at solutions like Quallace, which does vulnerability detection, patch management, baseline configuration assessment, and application scanning."*

This strategy aligns with the recommendations of the US National Institute of Standards and Technology (NIST), which emphasises the adoption of vulnerability management tools and processes to effectively manage risks (NIST, 2021).

Participant P20, with skills in network, threat, and vulnerability management, highlighted the challenges of patch management, particularly when it comes to remote devices:

> *"Another big one was patch management. So patch management remotely is very hard to do. Lots of organisations try to push it, but if you're at home. Off the network, some people don't log in."*

This aligned with Milson and Altan (2023), who also highlighted the difficulties of managing and patching remote devices outside the corporate network.

Participant P19, with skills in threat analysis, incident response, and network security expertise, emphasised the importance of prioritising patching based on vulnerability severity:

> *"So, each organisation has their own patch management policy, right? So that also determines when you fix your vulnerabilities that have been detected. And the house, how do you prioritise your patching because you can't patch everything at once because? - There could be a lot of vulnerabilities. So you need to patch on the severity of each vulnerability, you know."*

This perspective aligns with the existing literature on risk-based patch management (Koskenkorva, 2021). According to Koskenkorva (2021), risk-based patch management involves assessing the potential harm that each vulnerability could cause and addressing those with the highest potential impact first, recognising that not all vulnerabilities pose the same level of risk to an organisation and that resources should be allocated based on the severity of each vulnerability. The use of vulnerability management frameworks like the Common Vulnerability Scoring System (CVSS) supports this approach by assigning severity scores to vulnerabilities to guide prioritisation (Walkowski et al., 2021). By using a standardised scoring system, organisations can objectively evaluate the severity of vulnerabilities and prioritise their patching efforts accordingly.

4.9.6 Object common main theme 6: Policy development and enforcement

The development and enforcement of cybersecurity policies emerged as a crucial theme in the study, with participants emphasising the importance of establishing clear guidelines and protocols to govern employee behaviour and data protection practices. This emphasis on policy development and enforcement can be explained using Social Control Theory (SCT), which posits that individuals are motivated to adhere to rules and regulations when they believe in their legitimacy and perceive the potential consequences of non-compliance (Hirschi, 1969). It

is also noteworthy that the previous Community and Rules element referred to the policy framework, which served as a foundation for the organisation's governance. In contrast, the Object element here targets the policies, with the aim of making actionable steps to better align them with the evolving needs and priorities of the organisation. This refinement enables the organisation to effectively adapt its cyber management practices to stay ahead of emerging threats and opportunities.

Participant P1, acting head of IS governance, highlighted the significance of policy development during the COVID-19 pandemic:

> *"Yes, we had policies before - policy became quite important during the COVID timeframe because they couldn't link it to something that had been approved and signed off and was enforceable versus things that were left open for interpretation until it was actually needed."*

This statement underscores the importance of having clear, enforceable policies that create a sense of legitimacy and accountability, motivating individuals to comply.

Participant P2, a cybersecurity engineer, emphasised:

> "*So, for example, a lot of companies would do vaccinations for their employees as part of their policy, so if you send them an email, let them know that this has to do with getting your free COVID vaccination through this company."*

This statement can be aligned with Institutional Theory, which suggests that organisations conform to societal norms and expectations to gain legitimacy and ensure their survival (Meyer & Rowan, 1977).

Participant P4, a deputy director in protection services, mentioned the importance of implementing control measures to mitigate potential security risks, stating:

> *"We then had to quickly draft a policy that spoke to blocking all USB ports. Just to make sure that people no longer use them."*

This is an example of implementing a control measure to prevent malware and other types of threats. Research suggests that blocking USB (universal serial bus) ports is an effective way to prevent malware and other types of threats (Sun et al., 2021). By blocking these ports, organisations can effectively prevent these types of attacks.

Participant P7, a cybersecurity specialist, noted that *"We never implemented anything of that kind of any policies."* This statement can be explained by the theory of organisational slack, which suggests that organisations with sufficient resources are more likely to allocate resources to policy development and enforcement (Cyert & March, 1963). In contrast, organisations with limited resources may prioritise other operational aspects over policy implementation, resulting in potential gaps in cybersecurity measures.

In contrast, participant P13, a head of research development and innovation in cybersecurity, highlighted the importance of policy updates:

> *"Certain things about data classification and data handling in transit - had to be updated. So that was probably the most changes, but it's still the same policies as we had pre-covid, just updated to deal with the new norm."*

This resonates with the concept of policy feedback, which suggests that policy outcomes can influence subsequent policy decisions and adaptations (Moynihan & Soss, 2014). As organisations encounter new challenges and threats, feedback from existing policies can inform the need for updates and modifications to address emerging risks effectively. Participant P24 noted:

> *"We definitely had policies in place, that speaks acceptable use. They're basically providing a guideline in terms of how our employees can actually manage our data and our digital assets...".*

This quote aligns with the principles of social control theory, which suggests that individuals conform to societal norms due to their bonds with society and desire to avoid deviance (Hirschi, 2015). Policies on acceptable use outline guidelines and restrictions on employee conduct, reinforcing the societal norms of responsible data and asset management.

4.10 Outcome element

The outcome is the consequence of the object actions mentioned previously. The study focused on the "cybersecurity management activity" within the broader organisational context, encompassing various processes, practices, and systems implemented by organisations to protect their digital assets from cyber-threats. The findings of the study highlighted a positive shift in the cybersecurity landscape within SA organisations in response to the challenges posed by the COVID-19 pandemic. The outcomes mentioned by the participants align with the cyber

management actions mentioned in the Object element discussion and can be categorised into different themes.

4.10.1 Outcome common main theme 1: Cybersecurity awareness

The participants' responses in Table 4.4 highlight the importance of addressing various aspects of cybersecurity in SA.

Table 4.4: Participants' cybersecurity awareness responses

Participant Number	Object (cyber management actions)	Outcome
P1	Encouraging and supporting forums and initiatives that promote collaboration, particularly spearheaded by females, to create synergy and change cybersecurity perspectives.	*"There are a lot of people that are starting forums about cybersecurity, and amazingly, it's actually also females that are spearheading a lot of these forums. It's actually amazing to see people coming together like that. The fact that we have a common goal in mind means that we want to change the way we think. People behave and how cybersecurity is perceived for our country is actually quite an amazing thing to do."*
P9	Conducting widespread awareness campaigns to educate individuals about the potential risks irrespective of their personal possessions, emphasising the importance of cybersecurity practices.	*"There's a total lack of awareness. I believe we have a high penetration rate for mobile technology. People have access to the Internet, but it doesn't come with security awareness. People think they have nothing, so they won't be targeted by cybercriminals, and that should be the mistake because it's not about what they have, it's what they have access to."*
P29	Implementing comprehensive employee awareness and training programmes, establishing cybersecurity policies and procedures, conducting regular assessments and audits to assess employee understanding, and fostering a cybersecurity-conscious culture.	*"Lack of awareness amongst employees within organisations in South Africa makes us vulnerable."*
P2	The cybersecurity management activity that may have led to this potential increase in cybersecurity risks is the lack of or inadequate cybersecurity training and awareness for vulnerable populations	*"I believe people are becoming desperate because they don't have any money or jobs from covid, so there will be a lot more attempted and probably successful scams against elderly people. Vulnerable people, so to speak. But hopefully, by that stage, people will get a little bit more educated and understand, like, you know, don't fall for these things, don't share your banking information with other people."*
P19	Promoting a cybersecurity-first mindset within the organisation by integrating cybersecurity considerations and protocols at every level and making it a primary concern rather than an afterthought	*"..but I always ask about cybersecurity mindsets, you know, it's always an afterthought."*
P8	Enhancing cybersecurity knowledge and resource allocation within government departments, implementing stricter consequences for cybercriminals, and bolstering cybersecurity measures in the private sector.	*"Government departments and agencies lack basic knowledge and resources in cybersecurity. There are no significant consequences for cybercriminals operating within our country. Private sector companies are targeted due to the presence of valuable information and willingness to pay ransoms. Private sector companies are more likely to comply with cybersecurity measures."*

Source: Researcher's own

Participant P1 emphasises that encouraging collaboration and initiatives, particularly those spearheaded by females, can lead to a change in cybersecurity perspectives. Widespread awareness campaigns, as highlighted by participant P9, can educate individuals about the

potential risks and emphasise the importance of cybersecurity practices, regardless of their personal possessions.

Implementing comprehensive employee awareness and training programmes can foster a cybersecurity-conscious culture, reducing the vulnerability of organisations, as participant P29 notes. However, inadequate cybersecurity training and awareness for vulnerable populations, such as the elderly, can lead to an increase in cybersecurity risks, as participant P2 cautions. Promoting a cybersecurity-first mindset within organisations can integrate cybersecurity considerations and protocols at every level, making it a primary concern rather than an afterthought, as participant P19 suggests.

Enhancing cybersecurity knowledge and resource allocation within government departments is crucial for mitigating cyber-threats, as participant P8 emphasises. Stricter consequences for cybercriminals are also essential for deterring malicious activity, while bolstering cybersecurity measures in the private sector is critical for protecting sensitive information and systems. These outcomes align with the literature on cybersecurity awareness and education. Zhang et al. (2021) highlighted the importance of employee awareness and training programmes in reducing cybersecurity risks. The findings support the need for a comprehensive approach to cybersecurity, including government support, private sector engagement, and public awareness campaigns (Nagyfejeo & Von Solms, 2020). Overall, these outcomes emphasise the need for a multi-faceted approach to addressing cybersecurity challenges in SA.

4.10.2 Outcome common main theme 2: Cyber-threats mitigation

The outcomes of the various cyber management actions highlight the importance of strengthening cybersecurity practices in SA.

Table 4.5: Participants' cyber-threats mitigation responses

Participant Number	Object (cyber management actions)	Outcome
P19	The emphasis on using firewalls and changing default settings to protect systems led to the outcome of promoting multi-factor authentication implementation to prevent brute-force password attacks and ensure better security protocols for businesses.	*"..the bigger you are and the more your staff have on the Internet, at least make sure that you have firewalls that could protect those systems, and ensure that any default settings that are on those passwords are changed immediately so that... Whoever tries to brute force and give you your password cannot do that."*
P30	Capacity-building in cybersecurity management refers to the process of enhancing an organisation's capabilities to effectively prevent, detect, respond, and recover from cyber incidents. It involves developing the necessary knowledge, skills, and resources within an organisation to handle cybersecurity challenges proactively.	*"Capacity building beats them all."*
P29	Implementing secure remote access solutions, enforcing strong authentication measures, monitoring network traffic for potential threats, and providing necessary security training to remote workers.	*"..because of remote work, there was an enforcement of implementing additional security on a network level."*
P18	The focus on risk management led to the outcome of understanding cybersecurity as a crucial element that businesses need to be aware of and mitigate risk accordingly, especially through multi-factor authentication implementation.	*"..but I think businesses should really see it just as another form of risk management. I mean, that's why your risk management, executive committees, and cybersecurity just forms part of that. For business, they just need to be aware of the risks and either mitigate most of the risks or decide whether it's acceptable for the business."*
P6	Strengthening IT hygiene practices through regular audits, vulnerability assessments, and prompt configuration management, while ensuring adequate resources for security forensic investigations.	*"The very first thing is it hygiene. Misconfigurations. If we look at some of the big data breaches across the world, like horizon, yahoo, LinkedIn, Facebook, and all those data breaches, what the researchers have discovered, and it's the same thing that I've discovered over the years in South Africa, is that it takes about six to nine months before an attacker is first identified in the network. So when we look at, why is this the case? It's generally because one of our networks or devices is misconfigured"*
P21	The need for a framework or platform to share ideas and discuss cybersecurity threats led to the outcome of greater threat monitoring and analysis, which is crucial for keeping networks safe and secure.	*"The technology that we have to use is also increasing, and those technologies also have vulnerabilities that these attackers are trying to exploit. So it will go up and up and then we just need to... Have a framework or a location where we can meet and share ideas to solve problems."*

Participant Number	Object (cyber management actions)	Outcome
P28	Threat monitoring and analysis led to the outcome of focusing on breaking barriers on the defending side of cybersecurity and catching up with attackers through implementing improved cybersecurity measures.	*"Until companies on the defending side break that only then we will be able to start catching up on these attackers."*
P12	Incorporating cybersecurity as an integral part of business continuity plans and crisis response strategies to mitigate financial struggles caused by cyber incidents.	*"Other companies had the comfort of saying we're going to develop further. The other companies are hit by the pandemic and they say how do we react to this? Otherwise, we financially will start struggling and we might have to shut the lights off."*
P13	Promoting and supporting local cybersecurity companies, encouraging the development of innovative African solutions, and fostering collaborations between local and international cybersecurity ecosystems.	*"Well, one thing I've noticed is there's a lot more local companies and trying to address that as an office, they've also identified that. There is a shortcoming in trying to rely only on international tools for this, so there's a lot of very nice, African companies."*
P7	Inadequate investment in cybersecurity training and governance leads to diminishing effectiveness in security forensic measures.	*"On a red team level as attackers, I think I can foresee a lot more cybercrime coming. But on a security forensic level, unfortunately, it still seems like it's diminishing quiet, quite drastically."*
P14	Conducting cost-benefit analyses, assessing risks and vulnerabilities, and adopting a balanced approach to make informed decisions regarding investment in certain services and security enhancements.	*"But one of is budget's security is expensive... So it's kind of that trade offer, should we push more in terms of certain services, or should we try to ramp up our security, which is also costly."*
P25	Remote work cybersecurity training led to the outcome of promoting the priority of cybersecurity measures in digital ways of working to ensure protection from potential cyber threats.	*"Then we can only just continue from there and maybe implementing a lot to just make sure that in our way of working or in our path to being as digitally advanced as possible. Then we are protected or as secure as possible."*

Source: Researcher's own

Cyber management outcomes are crucial for ensuring the security and integrity of business systems. As highlighted by participant P19, emphasising firewalls and default settings can lead to multi-factor authentication implementation, thereby preventing brute-force attacks. Capacity building in cybersecurity management, as mentioned by participant P30, is essential for proactive handling of cyber challenges. Implementing secure remote access solutions, enforcing strong authentication measures, and providing necessary security training, as discussed by participant P29, can mitigate potential threats. Participants P18 and P6 emphasised the importance of risk management, highlighting the need to be aware of cybersecurity risks and mitigate them accordingly. Participant P21 stressed the need for a framework or platform to share ideas and discuss cybersecurity-threats, which led to greater threat monitoring and analysis. Participants P28 and P12 emphasised the importance of threat monitoring and analysis, as well as incorporating cybersecurity into business continuity plans and crisis response strategies.

Incorporating cybersecurity into business continuity plans and crisis response strategies can help mitigate financial struggles caused by cyber incidents, as highlighted by participant P12.

Participants P13 and P25 emphasised the importance of promoting local cybersecurity companies, encouraging the development of innovative African solutions, and fostering collaborations between local and international cybersecurity ecosystems. Finally, participants P7 and P14 highlighted the need for adequate investment in cybersecurity training and governance, as well as conducting cost-benefit analyses to make informed decisions regarding investment in certain services and security enhancements. Overall, these outcomes emphasise the importance of prioritising cybersecurity measures in digital ways of working, promoting the development of innovative African solutions, and fostering collaborations between local and international cybersecurity ecosystems (Lebogang et al., 2022).

4.10.3 Outcome common main theme 3: Cybersecurity advancements

The participants' responses highlight the importance of addressing the cybersecurity challenges faced by SA.

Table 4.6: Participants' cybersecurity advancements responses

Participant Number	Object (cyber management actions)	Outcome
P23	A focus on implementing system updates and patching led to the outcome of addressing cybersecurity issues related to lack of standardisation and awareness of cybersecurity protocols amongst businesses.	*"there's a lack of actual cybersecurity- our standards or most companies don't even follow a framework. They are basically clueless when it comes to how they need to protect their enterprise environment... I think that's a major factor, and also a lack of skills. There are not many cybersecurity professionals."*
P4	Enhancing skill development programmes, establishing proper governance frameworks and channels, and fostering a nationwide culture of cybersecurity awareness to mitigate targeted attacks.	*"I think the lack of skills, the lack of proper governance, documenting proper governance channels and the music that we are in emerging markets is definitely why we are being targeted. So it's creating a security wins culture nationwide, I think we lack a total awareness culture."*
P27	Continuously assessing the evolving cybersecurity landscape, adapting to emerging threats, keeping pace with technological advancements, and aligning cybersecurity strategies with the country's overall progress agenda.	*"...it all depends on the way that South Africa as a whole progresses or regresses."*
P11	Bridging the skills gap through training programmes, partnerships with educational institutions, and attracting cybersecurity professionals with competitive incentives.	*"You know, it could have to do with the skill shortage. That is definitely an issue for us as well, skills. So it's an issue."*
P16	Implementing data localisation measures and ensuring data sovereignty by requiring sensitive information to be stored and processed within the country's borders.	*"You still need all sensitive information to be protected within the country."*
P27	Internal assessments led to the outcome of recognising the need to keep skilled cybersecurity professionals in South Africa, who can positively contribute to improving cybersecurity frameworks and measures in the country.	*"I would say that it is going to get better. It can only get better from you... It's also about keeping the skills that we do have and the brain power and the analytical kind of mindsets, etc that we do have in the country."*
P5	Establishing a strong cybersecurity strategy, promoting cybersecurity awareness at the board level, investing in security skills development, and aligning cybersecurity with organisational objectives.	*"Companies will start to take cybersecurity seriously from board level to skill developments. Because at the moment, the companies paying at the leg to get subpar security skills because the market is dry and the international market is also not tapping into South Africa because the rates are a bit reasonable as compared to the western world."*

Source: Researcher's own

Participant P23 said that standardisation and awareness of cybersecurity protocols amongst businesses are crucial, citing the lack of actual cybersecurity and a shortage of skilled professionals. This underscores the need for a nationwide culture of cybersecurity awareness, as participant P4 stressed that enhancing skills development programmes, establishing proper governance frameworks, and fostering a culture of cybersecurity awareness are essential to mitigate targeted attacks.

To stay ahead of evolving threats, participant P27 emphasised the need to continuously assess the cybersecurity landscape and adapt to emerging risks. This requires aligning cybersecurity strategies with the country's overall progress agenda, as participant P27 highlighted. Participant P11 highlighted the need to bridge the skills gap through training programmes, partnerships with educational institutions, and attracting cybersecurity professionals with competitive incentives.

Participant P16 emphasised the importance of implementing data localisation measures and ensuring data sovereignty by requiring sensitive information to be stored and processed within SA's borders. This would not only protect local data but also keep skilled cybersecurity professionals in SA, who can positively contribute to improving cybersecurity frameworks and measures in the country. Finally, participant P5 suggested that companies will start to take cybersecurity seriously from board level to skills developments, as they are currently paying a premium for subpar security skills due to a shortage of skilled professionals.

This outcome is consistent with existing literature on the importance of addressing cybersecurity challenges in emerging countries. For example, a study by Pieterse (2021) found that cybersecurity is a critical issue for businesses operating in emerging countries, where there is a lack of awareness and skills amongst employees, leading to a heightened risk of data breaches and other security threats. Mannion (2020) found that data localisation is a critical issue in many emerging countries, where governments are imposing restrictions on data transfer to protect national security. The participants' responses highlight the importance of addressing these challenges in SA and emphasise the need for a comprehensive approach that includes skills development, governance frameworks, and data localisation measures.

4.11 Chapter 4 Summary

Chapter 4 provides an in-depth examination of findings related to cybersecurity management practices in South African organisations during the COVID-19 pandemic. It uncovers essential themes such as vulnerability assessment, challenges associated with digitisation, and the

increase in phishing and social engineering attacks, all of which are bolstered by participants' experiences and relevant literature. The chapter underscores the vital importance of policies, training, and tools in cultivating a cybersecurity-aware culture and mitigating cyber threats. Additionally, it emphasises the significance of community involvement and the division of labour in strengthening cybersecurity resilience. The utilisation of the Activity Theory Framework (ATF) throughout the analysis enhances the interpretation of the data by offering a structured approach to examining the interactions amongst various elements - including subjects, tools, and community dynamics - that influence cybersecurity practices. This context reaffirms the importance of the theoretical framework, effectively addressing the research questions by demonstrating how organisations can modify their strategies to navigate the complexities introduced by the pandemic. Overall, the findings reveal a notable transformation in the cybersecurity landscape, driven by the necessity to adapt to emerging threats and organisational challenges during the pandemic.

Chapter 5: Contradictions

Chapter 5 explores contradictions within Engström's ATF, uncovering tensions and challenges in addressing cybersecurity in organisations during the COVID-19 pandemic. The researcher had not set out to conduct research to initially find contradictions, but these insights provided new information, enriched the research and suggested ways to navigate cybersecurity management during those uncertain times, based on common views.

5.1 Primary Contradictions

The primary contradictions identified in this study concerning cybersecurity management aligned with existing literature findings, shedding light on critical challenges faced by organisations in safeguarding their digital assets (Cohen & Felson, 1979). The subject-tool contradiction underlined the importance of a proactive cybersecurity approach over reliance on basic tools like antivirus and firewall systems (Bandura & Walters, 1977). However, organisations continue to struggle with investing in comprehensive cybersecurity measures, indicating potential deficiencies in capable guardianship. The discrepancy between the emphasis on immediate action and the lack of investment in cybersecurity awareness raised concerns about organisations' priorities in addressing cybersecurity risks (Cornish & Clarke, 1989). The need for cost-benefit analyses to evaluate preventive measures' effectiveness was discussed, overlooking challenges in accurately quantifying potential cyber incident costs (Vavatsioulas, 2023). The focus on integrating preventive and reactive measures highlighted the need for coordinated cybersecurity strategies (Simon & Omar, 2020). However, further exploration is warranted concerning the practical implementation of such strategies and the trade-offs involved in prioritising one approach over another.

5.2 Secondary contradictions

The ATF in cybersecurity management identifies secondary contradictions in the division of labour, community collaboration, and tool use. These contradictions, based on theories like Strain Theory (Cornish & Clarke, 1989), emphasised the need for a well-defined division of labour that considers technical expertise, cybersecurity awareness, industry-specific vulnerabilities, and proactive measures to effectively address cybersecurity-threats.

Object-community-outcome relationships revealed challenges and discrepancies in cybersecurity practices, with some participants highlighting the lack of awareness, comprehensive strategies, and consequences for cybercriminals in SA. In the tool-community-outcome domain, contradictions arise due to varying priorities on tool selection and usage

amongst participants, emphasising the need for collaboration and shared understanding. This is understood in the context of Strain Theory, emphasising the importance of suitable tools and resources for incident response. Fostering open communication and collaboration can align perspectives and tool selection, leading to a more robust and integrated cybersecurity framework (Olaniyi et al., 2023).

5.3 Third contradictions

The subject-community-division of labour-outcome contradiction in SA organisations involves the conflict between personal and professional cybersecurity responsibilities, emphasising the importance of shared accountability and clearly defined roles for effective cybersecurity practices. This highlights the need for individuals to understand their cybersecurity duties, both in their personal lives and within their professional roles, to ensure better overall security outcomes (Corradini, 2020). The ATF uncovered inconsistencies in cybersecurity approaches exacerbated by the pandemic, highlighting the struggle to adapt to new measures and secure consistent cybersecurity strategies. The tool-division of labour-outcome contradiction showcases tensions surrounding tools, division of labour, and desired security outcomes, underscoring the crucial importance of investing in appropriate technologies that match cybersecurity goals. The study underscored the lower security maturity in SA, stressing the urgent requirement for increased commitment, capacity, skills, and laws to enhance cybersecurity practices.

5.4 Fourth contradictions

In the realm of quaternary contradictions within cybersecurity, one contradiction centres around collaborative efforts in the cybersecurity community against a backdrop of lacking comprehensive cybersecurity laws (Pylant, 2020). Another contradiction involves the necessity of training programmes amid existing skills gaps and governance challenges, illuminating the impact of social disorganisation within the cybersecurity landscape. The contrast between industry standards and a nationwide cybersecurity strategy highlights the strain between implementing cybersecurity goals without a comprehensive strategic framework (Agnew & White, 1992). Lastly, the challenge of policy implementation versus the emphasis on training programmes and proactive measures reveals a quandary encapsulating the interplay between reinforcement, modelling, and organisational culture in cybersecurity practices (Zwilling et al., 2022).

5.5 Chapter 5 Summary

Chapter 5 examines the contradictions inherent in Engström's Activity Theory Framework (ATF) as they pertain to cybersecurity management during the COVID-19 pandemic. It identifies the primary contradictions associated with proactive versus reactive approaches to cybersecurity, underscoring challenges related to investment and awareness. The secondary contradictions highlight the necessity for collaboration and clearly defined roles within cybersecurity practices. The chapter further addresses the third contradictions that reveal the tension between personal and professional cybersecurity responsibilities, emphasising the requirement for appropriate tools. Lastly, it investigates the fourth contradictions that expose the disconnect between industry standards and centralised cybersecurity strategies, as well as the challenges arising from skills gaps and social disorganisation.

Chapter 6: Conclusion

The conclusion provides a comprehensive analysis of COVID-19's impact on cybersecurity practices in SA, outlining vulnerabilities, challenges, and responses. It aims to enhance cybersecurity strategies by offering insights and recommendations to address evolving threats effectively in SA.

6.1 Primary research question: What are the COVID-19 effects on cybersecurity in organisations in SA?

The effects of COVID-19 on cybersecurity in organisations in SA have been significant, particularly in the context of the country's telecommunications infrastructure. The increased reliance on remote work during the pandemic has exposed vulnerabilities in Internet connectivity and network reliability (Tadesse & Muluye, 2020). These challenges in digital infrastructure had hindered organisations in SA from implementing and maintaining secure remote work environments, leaving them susceptible to cyber-threats and potential data breaches.

The pandemic has seen a rise in COVID-19-themed cyber-attacks targeting individuals and organisations in SA. Cybercriminals have taken advantage of the fear and uncertainty surrounding the pandemic to launch phishing campaigns and social engineering scams, often masquerading as reputable entities such as government bodies (Coetzee, 2022). These deceptive tactics aim to trick users into divulging sensitive information or unwittingly downloading malware, highlighting the need for heightened vigilance and robust security measures to combat such malicious activities effectively.

The economic repercussions of the pandemic have placed financial strain on many organisations in SA, forcing them to cut costs and reduce cybersecurity budgets. This financial pressure has made it difficult for companies to invest in comprehensive cybersecurity solutions and recruit skilled professionals to safeguard their digital assets (Chinka, 2023). Organisations may be more vulnerable to cyber-attacks and could face challenges in recovering from security breaches, underscoring the critical importance of prioritising cybersecurity measures even in times of financial hardship.

6.2 Secondary research question 1: How has COVID-19-induced remote work threatened cybersecurity in organisations?

The shift to remote work induced by COVID-19 has significantly heightened cybersecurity-threats in organisations in SA, with several unique challenges that set it apart from the global

landscape. One key aspect that makes SA unique is its socio-economic landscape, characterised by disparities in digital infrastructure and access. While remote work became a necessity for many organisations due to the pandemic, not all employees in SA have access to secure and reliable Internet connections or devices. This digital divide creates vulnerabilities that cybercriminals can exploit, targeting individuals who may not have the resources or expertise to implement robust cybersecurity measures (Renaud & Coles-Kemp, 2022).

SA faces persistent challenges related to cybercrime, with high levels of phishing attacks, and social engineering scams targeting organisations and individuals. The increased reliance on digital platforms for remote work has provided cybercriminals with more opportunities to launch sophisticated attacks, preying on unsuspecting employees who may not be adequately trained in cybersecurity awareness (Chawla et al., 2023).

The regulatory landscape in SA adds another layer of complexity to cybersecurity challenges. The POPI Act and other data protection regulations require organisations to adhere to stringent data privacy and security standards, imposing legal obligations to safeguard sensitive information. The shift to remote work has introduced new compliance risks, as employees handle and access data outside of secure office environments, potentially exposing organisations to regulatory penalties in case of data breaches.

6.3 Secondary research question 2: How has COVID-19 changed the way organisations practise cybersecurity awareness?

COVID-19 has reshaped the approach of SA organisations towards cybersecurity awareness. The pandemic prompted a rapid shift to remote work, increasing reliance on digital platforms and heightening the risk of cyber-threats. This forced organisations to prioritise cybersecurity awareness amongst employees, emphasising the importance of recognising and preventing potential risks. With the surge in phishing attacks and other cyber-threats exploiting the chaos of the pandemic, SA organisations have been compelled to enhance their cybersecurity training programmes and communication strategies. The focus has shifted towards promoting vigilance, secure practices, and implementing robust security measures to safeguard sensitive data and mitigate risks. The pandemic has accelerated the adoption of technologies like VPNs and MFA to bolster defences against cyber-threats.

This transformation in cybersecurity practices post-COVID-19 is in line with global trends, as organisations worldwide recognised the critical role of employee awareness in mitigating cyber risks (Okereafor & Adelaiye, 2020). By integrating interactive training modules, simulated phishing exercises, and gamified cybersecurity awareness programmes, SA organisations are

fostering a culture of cyber-resilience and empowering employees to actively contribute to the organisation's cybersecurity posture. This interactive approach not only enhances employee engagement but ensures that cybersecurity best practices are effectively communicated and internalised.

6.4 Secondary research question 3: By being based in SA, how have organisations become more appealing to COVID-19 cybersecurity-threats?

SA organisations are grappling with increased cybersecurity-threats due to economic instability, limited cybersecurity knowledge, and reliance on remote work during the COVID-19 pandemic. Studies by De Jager et al. (2023) and Olofinbiyi (2022), support the idea that SA lags in terms of cybersecurity understanding. As a result, cybercriminals have exploited the vulnerabilities in SA organisations, targeting them for data theft. To address these risks, organisations should focus on implementing secure remote work solutions, training employees to prevent and detect cyberattacks, developing incident response plans, and increasing investments in cybersecurity. To enhance cybersecurity in SA, it is crucial to allocate a larger budget for cybersecurity measures, implement advanced threat detection and prevention tools, and monitor and analyse network traffic. Developing a skilled cybersecurity workforce, establishing a national cybersecurity centre, and enhancing cybersecurity education and awareness are essential. SA can improve its cybersecurity maturity by creating a comprehensive cybersecurity strategy, fostering a security-focused culture within organisations, and implementing a continuous monitoring and improvement framework. Strengthening cybersecurity regulations and laws, increasing international cooperation and information-sharing, and enhancing public-private partnerships for cybersecurity initiatives are also necessary. By prioritising these measures, SA can improve its cybersecurity posture, protect against cyber-threats, and support the growth of its economy. Building a strong cybersecurity capacity requires a multi-faceted approach that addresses both the technical and human aspects of cybersecurity. This research contributed to the existing knowledge by providing localised insights and addressing the increased appeal of COVID-19 cybersecurity-threats in SA organisations.

6.5 Main objective 1

- The primary objective of this study was to analyse the effects of COVID-19 on cybersecurity practices within SA organisations, to detect potential vulnerabilities and devise efficient tactics to enhance cybersecurity and combat the difficulties arising from the pandemic.

The study analysed COVID-19's impact on SA organisations' cybersecurity practices, identifying potential vulnerabilities and devising effective strategies to improve security and mitigate pandemic-related challenges. The study highlights the rise in cyberattacks due to remote work, highlighting vulnerabilities like unsecured Wi-Fi networks and phishing attacks, urging for cybersecurity infrastructure investments. The recommendations for strengthening cybersecurity strategies in organisations include updating policies, increasing awareness training, evaluating staff proficiency, and improving incident response plans.

6.6. Limitations

The study employed Engström's ATF to examine cybersecurity ecosystem interactions during COVID-19, providing a comprehensive understanding of vulnerabilities in technology, individuals, and organisational practices. The research identified specific vulnerabilities in SA organisations' cybersecurity practices, and recommended solutions such as updating software, enhancing password management, and staff training. However, the study's limited data sources and focus on immediate pandemic impact may have narrowed its perspective on post-COVID-19 challenges and limited the generalisability of its findings to all SA organisations.

6.7. Implications for academia and significance of study for SA

The study undertook a comprehensive examination of the effects of COVID-19 on cybersecurity in SA organisations, yielding valuable insights into the cyber-threats, vulnerabilities, and organisational responses that emerged during this period. In this study, the ATF was employed as a theoretical lens to illuminate the intricate interplay within the cybersecurity ecosystem, thereby providing a nuanced understanding of the complex dynamics at play. By examining the effects of COVID-19 on cybersecurity in SA organisations, this study contributes to the burgeoning body of literature on pandemic-related cybersecurity concerns, ultimately informing the development of more effective strategies for mitigating these risks. By integrating these concepts with existing academic theory, the study benefited from the consolidation and integration of knowledge, thereby facilitating a more nuanced understanding of the complex relationships between cybersecurity, pandemic response, and crisis management. This study's findings have significant implications for the development of more effective policies, strategies, and practices that are informed by a deeper understanding of the underlying theoretical frameworks. Specifically, the research identifies vulnerabilities in SA organisations cybersecurity during and post-COVID-19, thereby highlighting important research gaps that require further investigation in future studies.

6.8 Chapter 6 Summary

In conclusion, this study significantly enhances the understanding of COVID-19's effects on cybersecurity practices within South African organisations by utilising Engström's Activity Theory Framework (ATF) as an analytical lens. The ATF enabled a detailed exploration of the multifaceted interactions amongst technology, individuals, and organisational processes during a crisis, revealing the specific vulnerabilities that arose during the pandemic. By connecting theoretical insights with empirical findings, this research addresses essential research questions and highlights the need for customised cybersecurity strategies that account for both immediate threats and long-term resilience. Ultimately, the integration of ATF contributes to the discourse on cybersecurity in the context of pandemics, paving the way for future studies aimed at strengthening defences against evolving cyber-threats in South Africa. This unique approach ensures that organisations can more effectively navigate the complexities of digital security in an increasingly unpredictable environment.

References

Abdulhameed, R.S. (2021). Crimes of threats and cyber extortion through social media: A comparative study. *Rigeo*, *11*(12). Available from: https://rigeo.org/menu-script/index.php/rigeo/article/view/1971/1969

African Union. (2020). *The Digital Transformation Strategy for Africa (2020-30)*. Available from: https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.pdf

Agarwal, R., & Prasad, J. (1998). The antecedents and consequents of user perceptions in information technology adoption. *Decision Support Systems*, *22*(1):15-29. https://doi.org/10.1016/S0167-9236(97)00006-7

Agnew, R., & White, H.R. (1992). An empirical test of general strain theory. *Criminology*, *30*(4):475-500. https://doi.org/10.1111/j.1745-9125.1992.tb01113.x

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2):179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Akdemir, N., & Lawless, C.J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6):1665-1687. https://doi.org/10.1108/INTR-10-2019-0400

Al-Ababneh, M. (2020). Linking ontology, epistemology and research methodology. *Science & Philosophy*, *8*(1):75-91. http://dx.doi.org/10.23756/sp.v8i1.500

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, *12*(10):168. https://doi.org/10.3390/fi12100168

Alhashmi, A.A., Darem, A., & Abawajy, J. (2021). Taxonomy of cybersecurity awareness delivery methods: A countermeasure for phishing threats. *International Journal of Advanced Computer Science and Applications*, *12*(10):29-35. https://dx.doi.org/10.14569/IJACSA.2021.0121004

Al-Hawamleh, A. (2024a). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, *15*(1), 1315-1331. http://dx.doi.org/10.12785/ijcds/150193

Al-Hawamleh, A.M. (2024b). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. *Digital Policy, Regulation and Governance*, *26*(3):317-336. https://doi.org/10.1108/DPRG-11-2023-0168

Al-Hawamleh, A.M.A., Alorfi, A.S.M., Al-Gasawneh, J.A., & Al-Rawashdeh, G. (2020). Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology*, *63*(5):7894-7899. Available from: https://solidstatetechnology.us/index.php/JSST/article/view/7202

Alhogail, A. (2021). Enhancing information security best practices sharing in virtual knowledge communities. *VINE Journal of Information and Knowledge Management Systems*, *51*(4):550-572. https://doi.org/10.1108/VJIKMS-01-2020-0009

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*(2021):563060. https://doi.org/10.3389/fcomp.2021.563060

Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S., & Khan, M.K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*(2020):137293-137311. https://doi.org/10.1109/ACCESS.2020.3011259

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(5):829-841. https://doi.org/10.1007/s00779-021-01551-2

AlShamsi, A., Mohaidat, J., Hinai, N.A., & Samy, A. (2020). Instructional and business continuity amid and beyond COVID-19 outbreak: A case study from the higher colleges of technology. *International Journal of Higher Education*, *9*(6):118-135. https://doi.org/10.5430/ijhe.v9n6p118

Amankwah-Amoah, J., Khan, Z., Wood, G., & Knight, G. (2021). COVID-19 and digitalization: The great acceleration. *Journal of Business Research*, *136*(2021):602-611. https://doi.org/10.1016/j.jbusres.2021.08.011

Angafor, G.N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and Privacy*, *3*(6):e126. https://doi.org/10.1002/spy2.126

Apakah, O. (2021). *Assessing the effects of Covid-19 on Africa's economic security, a case study of Kenya's hospitality and tourism sectors.* Published doctoral thesis, University of Nairobi. Available from: http://erepository.uonbi.ac.ke/handle/11295/160415.

Arab, M.S. (2020). Global surge in cybercrimes-Indian response and empirical evidence on need for a robust crime prevention system. *International Journal of Cyber Criminology*, *14*(2):497-507. https://doi.org/10.5281/zenodo.4772797

Arunprasad, P., Dey, C., Jebli, F., Manimuthu, A., & El Hathat, Z. (2022). Exploring the remote work challenges in the era of COVID-19 pandemic: review and application model. *Benchmarking: An International Journal*, *29*(10):3333-3355. https://doi.org/10.1108/BIJ-07-2021-0421

Ashraf, I., Park, Y., Hur, S., Kim, S.W., Alroobaea, R., Zikria, Y.B., & Nosheen, S. (2022). A survey on cyber security threats in IOT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2):2677-2690. https://doi.org/10.1109/TITS.2022.3164678

Bada, M., & Nurse, J.R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3):393-410. http://dx.doi.org/10.1108/ICS-07-2018-0080

Badamasi, B., Musa, S., & Umar, A.M.A. 2019. Qualitative case study of cybercrime types on Ahmadu Bello University's network. *International Journal of Information Processing and Communications*, *7*(2):83-99. Available from: http://hdl.handle.net/123456789/12289

Bandura, A. (1977). *Social learning theory*. New Jersey, USA: Prentice-Hall.

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist, 44*(9):1175–1184. https://doi.org/10.1037/0003-066X.44.9.1175

Bandura, A., & Walters, R.H. (1977). *Social learning theory* (Vol. 1). Englewood Cliffs: Prentice Hall.

Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. *Journal of Accounting and Public Policy*, *41*(6):106998. https://doi.org/10.1016/j.jaccpubpol.2022.106998

Bauchan, P.W. (2023). *A social ontological account of alienation and its place in the history of alienation theory*. Published doctoral thesis, Loyola University Chicago. Available from: https://ecommons.luc.edu/luc_diss/4008.

Baz, M., Alhakami, H., Agrawal, A., Baz, A., & Khan, R.A. (2021). Impact of COVID-19 pandemic: A cybersecurity perspective. *Intelligent Automation & Soft Computing*, *27*(3):641-652. http://dx.doi.org/10.32604/iasc.2021.015845

Belmabrouk, K. (2023). Cyber criminals and data privacy measures. In: N.Mateus-Coelho & M.M. Cruz-Cunha (eds.), *Contemporary challenges for cyber security and data privacy* (pp: 198-226). IGI Global. https://doi.org/10.4018/979-8-3693-1528-6

Bernal, J. (2009). Cybersecurity best practices: The principle of least privilege. *Journal of Information Security*, *15*(2):120-135.

Bernatzky, C., Costello, M. & Hawdon, J. (2021). Who produces online hate? An examination of the effects of self-control, social structure, & social learning. *American Journal of Criminal Justice*, *47*(2021):421–440. https://doi.org/10.1007/s12103-020-09597-3

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. Textbooks Collection. 3. Tampa, FL: University of South Florida. Available from: https://digitalcommons.usf.edu/oa_textbooks/3?utm_source=digitalcommons.usf.edu%2Foa_textbooks%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages

Bhowmik, S. (2023). The evolution of crime: The dynamic definition of crime as per society. *International Journal of Law Management and Humanities*, *6*(3):3638-3689. https://doij.org/10.10000/IJLMH.115284

Bispham, M., Creese, S., Dutton, W.H., Esteve-Gonzalez, P., & Goldsmith, M. (2021). *Cybersecurity in working from home: An exploratory study*. TPRC49: Proceedings of the 49th Research Conference on Communication, Information and Internet Policy. https://dx.doi.org/10.2139/ssrn.3897380

Blau, P.M. (1964). *Exchange and power in social life*. New York: Wiley

Borkovich, D.J. & Skovira, R.J. (2020). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems, 21*(4). http://dx.doi.org/10.48009/4_iis_2020_234-246

Bote, D. (2019). *The South African national cyber security policy framework: A critical analysis.* Unpublished doctoral thesis, North-West University, SA. Available from: http://hdl.handle.net/10394/33810

Boughrous, M., El Bakkali, H., & El Kandoussi, A. (2021, December). *The pandemic impact on organizations security and resiliency: the workflow satisfiability problem*. Proceedings of the International Conference on Hybrid Intelligent Systems. (pp: 321-329). Cham: Springer. http://dx.doi.org/10.1007/978-3-030-96305-7_30

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2006):77-101. https://doi.org/10.1191/1478088706qp063oa

Brosnan, M. (2021). Cyber-dependent crime, autism, and autistic-like traits. In: F.R. Volkmar, R. Loftin, A., Westphal & M. Woodbury-Smith (eds.), *Handbook of autism spectrum disorder and the law*. Cham: Springer. https://doi.org/10.1007/978-3-030-70913-6_10

Bryant, J., Holloway, K., Lough, O., & Willitts-King, B. (2020). Bridging humanitarian digital divides during Covid-19. *HPG briefing note. London: ODI.* Available from: https://odi.org/en/publications/bridginghumanitarian-digital-divides-during-covid-19/

Burdon, W.M., & Sorour, M.K. (2020). Institutional theory and evolution of 'a legitimate' compliance culture: The case of the UK financial service sector. *Journal of Business Ethics*, *162*(2020):47-80. https://doi.org/10.1007/s10551-018-3981-4

Cabanias, J.O. (2019). Communication within the workplace in the academics of De La Salle Medical and Health Sciences Institute: Basis for proposed communication strategic model. *British Journal of Medical & Health Sciences, 1*(1):1-9. Available from: http://www.jmhsci.org/wp-content/uploads/2019/07/BJMHS450003.pdf

Calandro, E. (2020). Observing global cyber norms nationally-The case of critical infrastructure protection in South Africa. https://dx.doi.org/10.2139/ssrn.3895156

Caldeira, C., RB de Souza, C., Machado, L., Perin, M., & Bjørn, P. (2023). Crisis readiness: revisiting the distance framework during the COVID-19 pandemic. *Computer Supported Cooperative Work, 32*(2):237-273. https://doi.org/10.1007/s10606-022-09427-6

Carcary, M. (2009). The research audit trial—enhancing trustworthiness in qualitative inquiry. *Electronic Journal of Business Research Methods*, *7*(1):11-24. Available from: https://academic-publishing.org/index.php/ejbrm/article/view/1239/1202

Carvalhaes, T., Markolf, S., Helmrich, A., Kim, Y., Li, R., Natarajan, M., Bondank, E., Ahmad, & Chester, M. (2020). COVID-19 as a harbinger of transforming infrastructure resilience. *Frontiers in Built Environment*, *6*(2020):148. https://doi.org/10.3389/fbuil.2020.00148

Chawla, R.K., Sodhi, J.S., & Singh, T. (2023). *Study of the need for effective cyber security trainings in India*. Proceedings of the International Conference on Data Management, Analytics & Innovation (pp: 697-720). Singapore: Springer Nature. Available from: https://scholar.google.com/scholar?oi=bibs&cluster=17265770834277134912&btnI=1&hl=en

Cherian, J., Gaikar, V., Paul, R., & Pech, R. (2021). Corporate culture and its impact on employees' attitude, performance, productivity, and behavior: An investigative analysis from selected organizations of the United Arab Emirates (UAE). *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(1):45. https://doi.org/10.3390/joitmc7010045

Cherns, A. (1976). The principles of sociotechnical design. *Human Relations*, *29*(8), 783-792. https://doi.org/10.1177/001872677602900806.

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1):1-11. http://dx.doi.org/10.4102/sajim.v23i1.1277

Chinka, S.G. (2023). *Influential factors in industrial cybersecurity: a systematic literature review and roadmap for future research*. Unpublished Master's dissertation, Tietotekniikka. Available from: https://urn.fi/URN:NBN:fi-fe20231218155196

Choi, J., Kruis, N.E., & Kim, J. (2019). Examining the links between general strain and control theories: An investigation of delinquency in South Korea. *Asian Journal of Criminology*, *14*(2019):201-221. https://doi.org/10.1007/s11417-019-09287-y

Chowdhury, M.A.A., & Fahim, M.H.K. (2020). An insight into the cybercrimes and cyber security measures in Bangladesh: Quest for operative legal remedies. *Solid State Technology*, *63*(6):22453-22468. Available from: http://solidstatetechnology.us/index.php/JSST/article/view/9095/6612

Cialdini, R.B. (1993). *Influence: The psychology of persuasion*. New York: HarperCollins.

Clarke, R.V., & Felson, M. (1993). Introduction: Criminology, routine activity, and rational choice. In: R.V. Clarke & M. Felson (eds). *Routine Activity and Rational Choice* (1-14). New Jersey, US: Transaction Publishers. https://doi.org/10.4324/9781315128788

Coetzee, A. (2022). *A conceptual model for phishing awareness: a South African study*. Unpublished Master's dissertation, University of Johannesburg. Available from: https://hdl.handle.net/10210/501360

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4):588-610. http://dx.doi.org/10.2307/2094589

Colicchia, C., Creazza, A., & Menachof, D.A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2):215-240. https://doi.org/10.1108/SCM-09-2017-0289

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2020). *Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies*. Apollo - University of Cambridge Repository. Available from: https://www.cl.cam.ac.uk/~bjc63/Crime_is_boring.pdf

Cornish, D.B., & Clarke, R.V. (1989). Crime specialisation, crime displacement and rational choice theory. In: H. Wegner, F. Lösel, & J. Haisch (eds.), *Criminal behavior and the justice system: Psychological perspectives* (pp: 103-117). Berlin: Springer Heidelberg. https://doi.org/10.1007/978-3-642-86017-1_7

Corradini, I. 2020. *Building a cybersecurity culture in Organizations: How to bridge the gap between people and digital technology*. Cham: Springer. https://doi.org/10.1007/978-3-030-43999-6

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10):13-21. http://dx.doi.org/10.22215/timreview/835

Cyert, R.M., & March, J.G. (1963). *A behavioral theory of the firm*. Englewood Cliffs, NJ: Prentice-Hall.

Darawsheh, W. (2014). Reflexivity in research: Promoting rigour, reliability and validity in qualitative research. *International Journal of Therapy and Rehabilitation*, *21*(12):560-568. https://doi.org/10.12968/ijtr.2014.21.12.560

D'Arcy, J., & Basoglu, A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems*, *23*(3):779-805. http://doi.org/10.17705/1jais.00740

Das, S., Wang, B., Kim, A., & Camp, L.J. (2020). *MFA is a necessary chore! Exploring user mental models of multi-factor authentication technologies*. Proceedings of the 53rd Hawaii International Conference on System Sciences. (pp. 1-10). Available from: http://hdl.handle.net/10125/64411

Delgado, M. F., Esenarro, D., Regalado, F. F. J., & Reátegui, M. D. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3 c TIC: cuadernos de desarrollo aplicados a las TIC*, 10(2), 123-141.

De Jager, M., Futcher, L., & Thomson, K.L. (2023). *An investigation into the cybersecurity skills gap in South Africa.* International Symposium on Human Aspects of Information Security and Assurance. (pp. 237-248). Cham: Springer Nature. http://dx.doi.org/10.1007/978-3-031-38530-8_19

Dewi, R. (2024). Automated infrastructure management and optimization for enhanced cybersecurity measures. *International Journal of Responsible Artificial Intelligence*, *14*(2):1-11. Available from: https://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/81

Di Sabato, V., & Savov, R. (2023). Training as a facilitator for Industry 4.0. *Revista de Gestão*. Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/REGE-12-2021-0208

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, *54*(1):76-92. https://doi.org/10.1177/00048658211003925

Durst, C., Wiser, F., Luber, S., & Wickramasinghe, N. (2020). Development of an activity theory-based framework for the analysis and design of socio-technical systems. *International Journal of Networking and Virtual Organisations*, *23*(3):261-293. http://dx.doi.org/10.1504/IJNVO.2020.10029277

Einler Larsson, L., & Qollakaj, K. (2023). *Cybersecurity of remote work migration: A study on the VPN security landscape post covid-19 outbreak*. Unpublished Bachelor's dissertation, Blekinge Institute of Technology, Karlskrona, Sweden. Available from: https://www.diva-portal.org/smash/get/diva2:1778036/FULLTEXT03.pdf

Engeström, Y. (1987). *Learning by expanding: An activity-theoretical approach to developmental research*. Cambridge: Cambridge University Press.

Engeström, Y. (1999). Activity theory and individual and social transformation. In: Y. Engeström, R. Miettinen & R.-L. Punamäki (eds.), *Perspectives on activity theory* (pp: 19–38). Cambridge USA: Cambridge University Press. (19-30).

Engeström, Y. (2001). Expansive learning at work: Toward an activity theoretical reconceptualization. *Journal of Education and Work, 14*(1):133-156. https://doi.org/10.1080/13639080020028747

Erdıvan, C. (2024). *Process, technology and human aspects of a security operations center*. Master of Science without thesis, Middle East Technical University. Available from: https://hdl.handle.net/11511/108246

Fagbule, O. (2023). *Cyber security training in small to medium-sized enterprises (SMEs): Exploring organisation culture and employee training needs.* Unpublished doctoral thesis, Bournemouth University.

Forliano, C., Orlandi, L.B., Zardini, A., & Rossignoli, C. (2023). Technological orientation and organizational resilience to Covid-19: The mediating role of strategy's digital maturity. *Technological Forecasting and Social Change, 188*(2023):122288. https://doi.org/10.1016/j.techfore.2022.122288

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

Geels, F.W. (2004). From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory. *Research Policy, 33*(6-7):897-920. https://doi.org/10.1016/j.respol.2004.01.015

Ghelani, D. (2022). *Cyber security, cyber threats, implications and future perspectives: A Review*. Authorea Preprints.

Gilgun, J.F. (2019). Deductive qualitative analysis and grounded theory: Sensitizing concepts and hypothesis-testing. In: K. Charmaz & A. Bryant (eds.), *The SAGE handbook of current developments in grounded theory*. (pp: 107-122). London: Sage.

Goutam, R.K. (2021). *Cybersecurity fundamentals: Understand the role of cybersecurity, its importance and modern techniques used by cybersecurity professionals.* English Edition. India: BPB Publications.

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data*, *4*(2021):583723. L https://doi.org/10.3389/fdata.2021.583723

Gulihar, P., & Gupta, B.B. (2020). Cooperative mechanisms for defending distributed denial of service (ddos) attacks. In: B.B. Gupta, G.M. Perez, D.P. Agrawal, & D. Gupta (eds.), *Handbook of computer networks and cyber security: Principles and paradigms (pp: 421-443)*. Cham: Springer Nature. https://doi.org/10.1007/978-3-030-22277-2

Hakimi, M., Fazil, A.W., Hakimi, F.M., Najieb, K., & Hakimi, S. (2024). Exploring the influences of cutting-edge technologies on operational efficiency, productivity, and financial profitability in Afghanistan's tourism sector. *Jurnal Riset Multidisiplin Dan Inovasi Teknologi*, *2*(01):168-83. http://dx.doi.org/10.59653/jimat.v2i01.417

Hasan, H., & Banna, S. (2012). The unit of analysis in IS theory: The case for activity. *Information Systems Foundations, 191*, 3-33.

Hashim, H.A., Salleh, Z., Shuhaimi, I., & Ismail, N.A.N. (2020). The risk of financial fraud: a management perspective. *Journal of Financial Crime*, *27*(4):1143-1159. https://doi.org/10.1108/JFC-04-2020-0062

Hatton, T., & Brown, C. (2021). Building adaptive business continuity plans: Practical tips on how to inject adaptiveness into continuity planning processes. *Journal of Business Continuity & Emergency Planning*, *15*(1):44-52. Available from: https://www.henrystewartpublications.com/sites/default/files/JBC15.1Building%20adaptive%20business%20continuity%20plans.pdf

Hay, C., & Ray, K. (2020). General strain theory and cybercrime. In: Holt, T., & Bossler, A. (eds). *The Palgrave handbook of international cybercrime and cyberdeviance*. Cham: Palgrave Macmillan.

He, W., Zhang, Z.J., & Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *International Journal of Information Management*, *57*(2021):102287. https://doi.org/10.1016/j.ijinfomgt.2020.102287

Hernández, C.A. (2023). The intersection of public health and cyber security: Lessons from the COVID-19 pandemic. *International Journal of Applied Health Care Analytics*, *8*(7):1-10. Available from: https://norislab.com/index.php/IJAHA/article/view/22

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. *IEEE Access*, *9*(2021):7152-7169. http://dx.doi.org/10.1109/ACCESS.2020.3048839

Hirschi, T. (1969*). Causes of delinquency*. Los Angeles: University of California Press.

Hirschi, T. (2015). *Social control theory: A control theory of delinquency*. In: F. Williams & M. McShane (eds.), *Criminology theory* (pp: 289-305). New York: Routledge.

Homans, G.C. (1958). Social behavior as exchange. *American Journal of Sociology, 63*(6):597-606. https://psycnet.apa.org/doi/10.1086/222355

Houston, L. (2019). *The relationship between organizational innovation, downsizing, and organizational size in small businesses.* Unpublished doctoral thesis, Capella University.

Hove, L. (2020). *Strategies used to mitigate social engineering attacks.* Unpublished doctoral thesis, Walden University. Available from: https://scholarworks.waldenu.edu/dissertations/9373

Hyde, K.F. (2000). Recognising deductive processes in qualitative research. *Qualitative Market Research: An International Journal*, *3*(2):82-90. https://doi.org/10.1108/13522750010322089

Iyamu, T., & Shaanika, I. (2019). The use of activity theory to guide information systems research. *Education and Information Technologies*, *24*(2019):165-180. https://doi.org/10.1007/s10639-018-9764-9

Jha, A., & Jha, A. (2023). Securing tomorrow's urban frontiers: A holistic approach to cybersecurity in smart cities. *Information System and Smart City*, *3*(1). https://doi.org/10.59400/issc.v3i1.41

Jimmy, F.N.U. (2024). Cybersecurity vulnerabilities and remediation through cloud security tools. *Journal of Artificial Intelligence General science, 2*(1):129-171. https://doi.org/10.60087/jaigs.vol03.issue01.p233

Johns, E. (2020). Cyber security breaches survey 2020. *Department for Digital, Culture, Media & Sport, 4*(1):1-4. Available from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

Johnson, R.B. & Christensen, L. (2017). *Educational research: Quantitative, qualitative, and mixed approaches*. Thousand Oaks, CA: Sage.

Jones, A. (2022). *Security posture: A systematic review of cyber threats and proactive security*. Senior thesis, Liberty University. Available from: https://digitalcommons.liberty.edu/honors/1147

Jordan, C.A. (2022). *Exploring the cybersecurity skills gap: A qualitative study of recruitment and retention from a human resource management perspective.* Unpublished doctoral thesis, Northcentral University.

Kalajžić, I. (2019). *Cybersecurity-the threat of social engineering*. Unpublished doctoral thesis, University of Zagreb.

Kam, H.J., & Shang, Y. (2019). *Improving cybersecurity learning: An integration of cyber offense and cyber defense*. Proceedings of PACIS 2019 177. Available from: https://aisel.aisnet.org/pacis2019/177

Kaptelinin, V., & Nardi, B.A. 2006. Activity theory in a nutshell. In: V. Kaptelenin & B.A. Nardi (eds.), *Acting with technology: Activity theory and interaction design* (pp: 29-72). Cambridge, MA: MIT Press. https://doi.org/10.1080/10749039.2017.1393089

Karakasilioti, G.M. (2024). *Supporting the digital operational resilience of the financial sector: The EU's Digital Operational Resilience Act.* Unpublished Master's thesis, Πανεπιστήμιο Πειραιώς. http://dx.doi.org/10.26267/unipi_dione/3695

Karanasios, S. (2018). Toward a unified view of technology and activity: The contribution of activity theory to information systems research. *Information Technology & People*, *31*(1):134-155. http://dx.doi.org/10.1108/ITP-04-2016-0074

Karjalainen, M., & Ojala, A.L. (2023). Authentic learning environments for in-service training in cybersecurity: A qualitative study. *International Journal of Continuing Engineering Education and Life Long Learning*, *33*(1):128-147. https://doi.org/10.1504/ijceell.2023.10041126

Kaushik, M., & Guleria, N. (2020). The impact of pandemic COVID-19 in workplace. *European Journal of Business and Management*, *12*(15):1-10. http://dx.doi.org/10.7176/EJBM/12-15-02

Khatri, K.K. (2020). Research paradigm: A philosophy of educational research. *International Journal of English Literature and Social Sciences*, *5*(5):1435-1440. https://dx.doi.org/10.22161/ijels.55.15

Khiralla, F.A.M. (2020). Statistics of cybercrime from 2016 to the first half of 2020. *Int. J. Comput. Sci. Netw.*, *9*(5):252-261. http://dx.doi.org/10.13140/RG.2.2.30131.66088

Kolb, D.A. (1984). *Experiential learning: Experience as the source of learning and development*. New Jersey: Prentice-Hall.

Koskenkorva, H. (2021). *The role of security patch management in vulnerability management*. Unpublished Master's thesis, South-Eastern Finland University of Applied Sciences. Available from: https://urn.fi/URN:NBN:fi:amk-2021120924851

Kour, R., Patwardhan, A., Thaduri, A., & Karim, R. (2023). *A review on cybersecurity in railways.* Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, *237*(1):3-20. https://doi.org/10.1177/09544097221089389

Kritzinger, E. (2020). Improving cybersafety maturity of South African schools. *Information*, *11*(10):471. https://doi.org/10.3390/info11100471

Kritzinger, E., Da Veiga, A., & van Staden, W. (2023). Measuring organizational information security awareness in South Africa. *Information Security Journal: A Global Perspective*, *32*(2):120-133. https://doi.org/10.1080/19393555.2022.2077265

Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach*. Toronto: University of Toronto Press.

Kunduru, A.R. (2023). Industry best practices on implementing oracle cloud ERP security. *International Journal of Computer Trends and Technology*, *71*(6):1-8. https://doi.org/10.14445/22312803/IJCTT-V71I6P101

Kuutti, K. (1996). 2. Activity theory as a potential framework for human-computer interaction research. In: A. Nardi (ed.), *Context and consciousness: Activity theory and human-computer interaction* (pp: 9-22). Cambridge, MA: MIT Press.

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*(2021):102248. https://doi.org/10.1016/j.cose.2021.102248

Lang, M., Connolly, L., Taylor, P., & Corner, P. J. (2023). The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks. *Digital Threats: Research and Practice*, 4(4), 1-22. https://doi.org/10.1145/3558006

Lave, J. & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge: Cambridge University Press.

Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating cybersecurity strategies in Africa. In: M. Dawson, O. Tabona & T. Maupong (eds.), *Cybersecurity capabilities in developing nations and its impact on global security* (pp: 1-19). IGI Global. http://dx.doi.org/10.4018/978-1-7998-8693-8.ch001

Leonardi, P.M. (2012). Materiality, sociomateriality, and socio-technical systems: What do these terms mean? How are they different? Do we need them? *Materiality and Organizing: Social Interaction in a Technological World*, *25*(10):1093. http://dx.doi.org/10.2139/ssrn.2129878

Leontiev, A.N. (1978). *Activity, consciousness, and personality*. Englewood Cliffs, NJ: Prentice Hall.

Liang, P., Wu, Y., Xu, Z., Xiao, S., & Yuan, J. (2024). Enhancing security in devops by integrating artificial intelligence and machine learning. *Journal of Theory and Practice of Engineering Science*, *4*(02):31-37. http://dx.doi.org/10.53469/jtpes.2024.04(02).05

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Journal of Entrepreneurship and Sustainability Issues*, *4*(4):559-573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

Loh Joey, K. (2021). *The strategic use of microlearning as a training approach for the purpose of workforce skills development in multinational corporations*. Published Master's dissertation, Zurich University of Applied Sciences. Available from: https://digitalcollection.zhaw.ch/handle/11475/24663

Longo, J. (2023). *Large v small organization software development: Are software development best practices one-size fits all?* Unpublished Master's dissertation: George Mason University. Available from: https://mars.gmu.edu/server/api/core/bitstreams/013c3c09-8ed1-4f5d-942a-9f9969856a50/content

Lythreatis, S., Singh, S.K., & El-Kassar, A.N. (2022). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*, *175*(2022):121359. https://doi.org/10.1016/j.techfore.2021.121359

Maathuis, C., & Chockalingam, S. (2022). *Victim versus offender: Behaviour modelling during Covid-19 pandemic cyber-attacks*. Proceedings of the 32nd European Safety and Reliability Conference (ESREL). Dublin, Ireland. http://dx.doi.org/10.3850/978-981-18-5183-4_S20-01-112-cd

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education*, *9*(3):3351-33514. Available from: http://ojs.aishe.org/index.php/aishe-j/article/view/335

Mahanta, K., & Maringanti, H.B. (2023). Social engineering attacks and countermeasures. In: K. Kaushik & A. Bhardwaj (eds.), *Perspectives on ethical hacking and penetration testing* (pp: 307-337). IGI Global. https://doi.org/10.4018/978-1-6684-8218-6

Maimon, D., & Louderback, E.R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*(2019):191-216. https://doi.org/10.1146/annurev-criminol-032317-092057

Malatji, M., Marnewick, A.L., & von Solms, S. (2020). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability, 13*(1):291. https://doi.org/10.3390/su13010291

Malik, P., & Garg, P. (2020). Learning organization and work engagement: The mediating role of employee resilience. *International Journal of Human Resource Management, 31*(8):1071-1094. https://doi.org/10.1080/09585192.2017.1396549

Mannion, C. (2020). Data imperialism: The GDPR's disastrous impact on Africa's E-commerce markets. *Vand. J. Transnat'l L., 53*(2020):685. Available from: https://scholarship.law.vanderbilt.edu/vjtl/vol53/iss2/6

Marshall, M.N. (1996). Sampling for qualitative research. *Family Practice, 13*(6):522-525. https://doi.org/10.1093/fampra/13.6.522

Mbanaso, U.M., Abrahams, L., & Okafor, K.C. (2023). Research philosophy, design and methodology. In: U.M. Mbanaso, L. Abrahams & K.C. Okafor (eds.), *Research techniques for computer science, information systems and cybersecurity* (pp: 81-113). Cham: Springer Nature. http://dx.doi.org/10.1007/978-3-031-30031-8

Merton, R.K. (1936). The unanticipated consequences of purposive social action. *American Sociological Review, 1*(6):894-904. https://doi.org/10.2307/2084615

Meyer, J.W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2):340-363. Available from: http://www.jstor.org/stable/2778293?origin=JSTOR-pdf

Milson, S., & Altan, B. (2023). *Cybersecurity in remote work environments: Challenges and best practices.* (No. 11614). EasyChair. Available from: https://easychair.org/publications/preprint/9lj5

Minnaar, A. (2020). Gone phishing: the cynical and opportunistic exploitation of the Coronavirus pandemic by cybercriminals. *Acta Criminologica: African Journal of Criminology & Victimology*, *33*(3):28-53. Available from: https://hdl.handle.net/10520/ejc-crim-v33-n3-a3

Mitcham, Z.S. (2024). *Key security concepts that all CISOs should know-cyber guardians: A CISO's guide to protecting the digital world*. Sudbury, MA: eBookIt.com.

Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). Analysis of the human factor in cybersecurity: Identifying and preventing social engineering attacks in financial institution. *IEEE.* http://dx.doi.org/10.13140/RG.2.2.35640.52489

Morrison, S. (2022). *Malware architects and rational choice: a case study analysis of three cyber-offenders*. Unpublished doctoral thesis, Macquarie University. Available from: http://hdl.handle.net/1959.14/1267960

Motulsky, S.L. (2021). Is member checking the gold standard of quality in qualitative research? *Qualitative Psychology*, *8*(3):389. http://dx.doi.org/10.1037/qup0000215

Moynihan, D.P., & Soss, J. (2014). Policy feedback and the politics of administration. *Public Administration Review*, *74*(3):320-332. https://doi.org/10.1111/puar.12200

Mphatheni, M.R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(4):384-396. https://doi.org/10.20525/ijrbs.v11i4.1714

Mughal, A.A. (2020). Cyber-attacks on OSI layers: Understanding the threat landscape. *Journal of Humanities and Applied Science Research, 3*(1):1-18. Available from: https://orcid.org/0009-0006-8460-8006

Mungo, J. (2023). Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks. *Journal of Cyber Security Technology*, *8*(2):71-119. https://doi.org/10.1080/23742917.2023.2244210

Mursu, Á., Luukkonen, I., Toivanen, M., & Korpela, M. (2007). Activity theory in information systems research and practice: Theoretical underpinnings for an information systems development model. *Information Research: an international electronic journal*, *12*(3):2006-2007. Available from: https://files.eric.ed.gov/fulltext/EJ1104804.pdf

Musuva, P. (2019). *A multi-dimensional model for determining susceptibility to unintentional insider threats: The case of social engineering through phishing. Unpublished* doctoral thesis, University of Nairobi.

Mwangi, E. (2024). *A systematic review of secure browsing habits: Mitigating online risks*. Authorea Preprints. https://doi.org/10.22541/au.170708930.00027957/v1

Nagyfejeo, E., & Von Solms, B. (2020). Why do national cybersecurity awareness programmes often fail? *International Journal of Information Security and Cybercrime, 9*(2):18-27. Available from: https://www.ijisc.com/year-2020-issue-2-article-3/

Nardi, B.A. (1996). Studying context: A comparison of activity theory, situated action models, and distributed cognition. In B.A. Nardi (ed.), *Context and consciousness: Activity theory and human–computer interaction* (69–102). Cambridge, MA; The MIT Press. https://doi.org/10.7551/mitpress/2137.001.0001

Ndemo, B. (2021). *Digital transformation and cyberstability: Effects on economic development in Africa*. Available from: https://hcss.nl/wp-content/uploads/2021/09/Digital-Transformation-and-Cyberstability-Effects-on-Economic-Development-in-Africa.pdf

Neuman, D. (2014). Qualitative research in educational communications and technology: A brief introduction to principles and procedures. *Journal of Computing in Higher Education*, *26*(2014):69-86. http://dx.doi.org/10.1007/s12528-014-9078-x

Ngo, F.T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious software threats. In: T. Holt, & A. Bossler (eds.), *The Palgrave handbook of international cybercrime and cyberdeviance.* Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3

Ning, X., & Jiang, J. (2022). Defense-in-depth against insider attacks in cyber-physical systems. *Internet of Things and Cyber-Physical Systems*, *2*(2022):203-211. https://doi.org/10.1016/j.iotcps.2022.12.001

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(1):49-72. https://doi.org/10.2478/hjbpa-2022-0003

Nwankwo, W., Kizito, A.E., Adigwe, W., Nwankwo, C.P., Uwadia, F., & Mande, S. (2022). *A community cloud-based store for forensic operations in cybercrime control*. 2022 5th Information Technology for Education and Development (ITED) (1-8). https://doi.org/10.1109/ITED56637.2022.10051615

Nyre-Yu, M.M. (2019). *Determining system requirements for human-machine integration in cyber security incident response*. Unpublished doctoral thesis, Purdue University. https://doi.org/10.25394/PGS.10014803.v1

Ogbanufe, O., Kim, D.J., & Jones, M.C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & Management*, *58*(7):103507. https://doi.org/10.1016/j.im.2021.103507

Okereafor, K., & Adelaiye, O. (2020). Randomized cyber-attack simulation model: a cybersecurity mitigation proposal for post covid-19 digital era. *International Journal of Recent Engineering Research and Development*, *5*(07):61-72. https://doi.org/10.6084/m9.figshare.12739163.v1

Olaniyi, O.O., Ugonnia, J.C., Olaniyi, F.G., Arigbabu, A.T., & Adigwe, C.S. (2024). Digital collaborative tools, strategic communication, and social capital: Unveiling the impact of digital transformation on organizational dynamics. *Asian Journal of Research in Computer Science*, *17*(5):140-156. http://dx.doi.org/10.9734/ajrcos/2024/v17i5444

Olawale, O., Ajayi, F.A., Udeh, C.A., & Odejide, O.A. (2024). Remote work policies for IT professionals: Review of current practices and future trends. *International Journal of Management & Entrepreneurship Research*, *6*(4):1236-1258. http://dx.doi.org/10.51594/ijmer.v6i4.1056

Ollerenshaw, J.A., & Creswell, J.W. (2002). Narrative research: A comparison of two restorying data analysis approaches. *Qualitative Inquiry*, *8*(3):329-347. https://doi.org/10.1177/10778004008003008

Olofinbiyi, S.A. (2022). A reassessment of public awareness and legislative framework on cybersecurity in South Africa. *ScienceRise: Juridical Science, 2*(20):34-42. http://dx.doi.org/10.15587/2523-4153.2022.259764

Omoyiola, B.O., & Mckeeby, J. (2023). Strategies For Implementing Cybersecurity Policies in Organizations (A Case Study of West African Organizations). *SSRN Electronic Journal, March 2023.* https://dx.doi.org/10.2139/ssrn.4395723

Orlikowski, W. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science*, *11*(4):404-428. Available from: https://www.jstor.org/stable/2640412.

Orunsolu, A.A., Sodiya, A.S., & Akinwale, A.T. (2022). A predictive model for phishing detection. *Journal of King Saud University-Computer and Information Sciences*, *34*(2):232-247. https://doi.org/10.1016/j.jksuci.2019.12.005

Østby, G., & Kowalski, S.J. (2022). *Organizational learning with crises–triple loop learning in cyber security exercises*. EDULEARN22 Proceedings (5215-5224). IATED. Available from: https://hdl.handle.net/11250/3042637

Ostrom, E., & Hess, C. (2011). Private and common property rights. In: A. Marciano & G.B. Ramello (eds.), *Encyclopedia of law and economics*. Gloucestershire, UK: Edward Elgar. https://doi.org/10.1007/978-1-4614-7753-2

Pahl-Wostl, C. (2007). Transitions towards adaptive management of water facing climate and global change. *Water Resources Management*, *21*(2007):49-62. https://doi.org/10.1007/s11269-006-9040-4

Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*(2020):102171. https://doi.org/10.1016%2Fj.ijinfomgt.2020.102171

Parsola, J. (2022). Cybersecurity risk assessment and management for organizational security. *NeuroQuantology*, *20*(5):5330. Available from: https://www.neuroquantology.com/media/article_pdfs/1037.pdf

PasswordManagers. 2020. *Cybersecurity Exposure Index 2020*. Password Managers. [online]. Available at: https://passwordmanagers.co/cybersecurity-exposure-index/

Paternoster, R. (2019). How much do we really know about criminal deterrence*? Journal of Criminal Law and Criminology*, *100*(3):765-823. http://dx.doi.org/10.2307/25766109

Patton, M.Q. (1987). *How to use qualitative methods in evaluation* (No. 4). CSE Program Evaluation Kit. Thousand Oaks, CA: Sage.

Pervin, N., & Mokhtar, M. (2022). The interpretivist research paradigm: A subjective notion of a social context. *International Journal of Academic Research in Progressive Education and Development*, *11*(2):419-428. http://dx.doi.org/10.6007/IJARPED/v11-i2/12938

Pickard, A.J. (2007). *Research methods in information*. London: Facet.

Piduru, B.R. (2022). Cloud computing and public sector transformation: Revolutionizing governmental services and operations. *Journal of Artificial Intelligence & Cloud Computing*, *1*(3):1-4. https://doi.org/10.47363/JAICC/2022(1)192

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *African Journal of Information and Communication*, *28*(2021):1-21. http://dx.doi.org/10.23962/10539/32213

Popescu, A.D. (2021). *Non-fungible tokens (nft)–innovation beyond the craze*. In 5th International Conference on Innovation in Business, Economics and Marketing Research (Vol. 32).

Prasad, R., & Rohokale, V. (2020). *Malware, cyber security: The lifeline of information and communication technology*. Cham: Springer.

Protrka, N. (2021). Cybercrime. In: M. Rycroft & L. Brine (eds.), *Modern police leadership* (pp: 143-155). Cham: Springer.

Pylant, A.C. (2020). *Initiating a collaborative cybersecurity governance framework at the state level*. Unpublished doctoral thesis, West Chester University.

Rakha, N.A. (2023). Ensuring cyber-security in remote workforce: Legal implications and international best practices. *International Journal of Law and Policy, 1*(3). https://doi.org/10.59022/ijlp.43

Rantalaiho, V. (2024). *Technical implementation and operational enhancements of a vulnerability management tool in an organization*. Unpublished Bachelor's dissertation, Turku University of Applied Sciences. Available from: https://urn.fi/URN:NBN:fi:amk-202404106189

Rejeb, A., Rejeb, K., & Keogh, J.G. (2021). Cryptocurrencies in modern finance: a literature review. *Etikonomi*, *20*(1):93-118. http://dx.doi.org/10.15408/etk.v20i1.169111

Renaud, K., & Coles-Kemp, L. (2022). Accessible and inclusive cyber security: a nuanced and complex challenge. *SN Computer Science*, *3*(5):346. https://doi.org/10.1007/s42979-022-01239-1

Reurink, A. (2019). Financial fraud: A literature review. *Journal of Economic Surveys*, *32*(5):1292-1325. https://doi.org/10.1111/joes.12294

Rindfleisch, A., Malter, A.J., Ganesan, S., & Moorman, C. (2008). Cross-sectional versus longitudinal survey research: Concepts, findings, and guidelines. *Journal of Marketing Research*, *45*(3):261-279. https://doi.org/10.1509/jmkr.45.3.261

Roberts, L.E. (2020). *Opening academia: An activity theory analysis of how academics learn and do openness*. Unpublished doctoral thesis: North Carolina State University.

Rodgers, B.L., & Cowles, K.V. (1993). The qualitative research audit trail: A complex collection of documentation. *Research in Nursing & Health, 16*(3):219-226. https://doi.org/10.1002/nur.4770160309

Roepke, R., Koehler, K., Drury, V., Schroeder, U., Wolf, M.R., & Meyer, U. (2020). *A pond full of phishing games-analysis of learning games for anti-phishing education*. Model-driven Simulation and Training Environments for Cybersecurity: Second International Workshop, MSTEC 2020, Guildford, UK, September 14–18, 2020, Revised Selected Papers 2. (41-60). https://doi.org/10.1007/978-3-030-62433-0_3

Ryan, K.O. (2020). Urban killing fields: International humanitarian law, gang violence, and armed conflict on the streets of El Salvador. *International and Comparative Law Review*, *20*(1):97-126. https://doi.org/10.2478/iclr-2020-0005

Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E., & Alabbad, D.A. (2023a). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15):6666. https://doi.org/10.3390/s23156666

Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H., & Almuhaideb, A.M. (2023b). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16):7273. https://doi.org/10.3390/s23167273

Safitra, M.F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18):13369. https://doi.org/10.3390/su151813369

Sala, E. & Martiri, E. (2023). ADR Project Planning TO Increase Cyber Security Awareness of Mobile Device Users. *International Journal on Technical and Physical Problems of Engineering (IJTPE), 15,* 327-333.

Saleous, H., Ismail, M., AlDaajeh, S.H., Madathil, N., Alrabaee, S., Choo, K.K.R., & Al-Qirim, N. (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks, 9*(1):211-222. https://doi.org/10.1016/j.dcan.2022.06.005

Saltzer, J.H., & Schroeder, M.D. 1975. The protection of information in computer systems. *Proceedings of the IEEE, 63*(9):1278-1308. https://doi.org/10.1109/PROC.1975.9939

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. New Jersey: Pearson Education.

Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, *23*(4):2525-2556. http://dx.doi.org/10.1109/COMST.2021.3117338

Sekgololo, M.J. (2024). University of Johannesburg Institutional Repository Cybersecurity Output: 2015-2021 Interdisciplinary Study. *Journal of Cybersecurity Education, Research and Practice,* 1(2024):16. Available from: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/16/

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6):539-550. https://doi.org/10.1080/08874417.2020.1812134

Shavell, S. (1992). Economic analysis of threats and their illegality: Blackmail, extortion, and robbery. *U. Pa. L. Rev.*, *141*(1992):1877-1903. http://doi.org/10.2307/3312577

Shaw, C.R., & McKay, H.D. (1942). *Juvenile delinquency and urban areas: A study of rates of delinquency in relation to differential characteristics of local communities in American cities*. Chicago: University of Chicago Press.

Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. *Computer Fraud & Security*, *1*(2021):14-19. https://doi.org/10.1016/S1361-3723(21)00009-9

Shingange, J.G. (2022). *Problematizing the South African cybersecurity policy landscape*. Unpublished doctoral thesis, Stellenbosch University.

Shufutinsky, A. (2020). Employing use of self for transparency, rigor, trustworthiness, and credibility in qualitative organizational research methods. *Organization Development Review*, *52*(1), 50-58.

Sikder, A.S., & Islam, M.R. (2023). Enhancing cyber-resilience within Bangladesh's legal framework: Evaluating preparedness and mitigation strategies against technologically-driven threats. *International Journal of Imminent Science & Technology*, *1*(1):40-57. http://dx.doi.org/10.13140/RG.2.2.10896.99842

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*(1):161-171. https://doi.org/10.1016/j.ejor.2019.09.017

Singh, H.P., & Alshammari, T.S. (2020). An institutional theory perspective on developing a cyber security legal framework: a case of Saudi Arabia. *Beijing L. Rev.*, *11*(3):637–650. https://doi.org/10.4236/blr.2020.113039

Slonka, K., Mishra, S., Draus, P., & Bromall, N. (2023). Measurement, reporting, and monitoring in organizational security governance from the security professional's perspective. *Cybersecurity Pedagogy & Practice Journal*, 2(1):38-84.

Sol, K., & Heng, K. (2022). Understanding epistemology and its key approaches in research. *Cambodian Journal of Educational Research*, *2*(2):80-99. https://doi.org/10.62037/cjer.2022.02.02.05

South Africa. 2013. *Protection of Personal Information Act number 4 of 2013*. Available from: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Stalans, L.J., & Donner, C.M. (2018). Explaining why cybercrime occurs: Criminological and psychological theories. In: H. Jahankhani (ed.), *Cyber criminology: Advanced sciences and technologies for security applications.* Cham: Springer Nature. http://dx.doi.org/10.1007/978-3-319-97181-0_2

Stebbins, R.A. (2001). What is exploration? *Exploratory Research in the Social Sciences*, *48*(2001):2-17. https://doi.org/10.4135/9781412984249

Steinmetz, K.F. 2021. Hacking and hacktivism. In: R. Atkinson & T. Ayres (eds.), *Shades of deviance*. London: Routledge.

Stigler, G.J., & Becker, G.S. (1977). De Gustibus Non Est Disputandum. *American Economic Review, 67*(2):76–90. Available from: https://www.jstor.org/stable/1807222

Stine, K., Quinn, S., Witte, G., & Gardner, R. (2020). Integrating cybersecurity and enterprise risk management (ERM). *National Institute of Standards and Technology*, National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8286

Sucheran, R. (2022). The COVID-19 pandemic and guesthouses in South Africa: Economic impacts and recovery measures. *Development Southern Africa*, *39*(1):35-50. https://doi.org/10.1080/0376835X.2021.2003758

Sun, C., Lu, J., & Liu, Y. (2021). Analysis and prevention of information security of USB. *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)* (pp. 25-32). IEEE. https://doi.org/10.1109/EIECS53707.2021.9588135

Sungkur, R.K., & Maharaj, M.S. (2021). Design and implementation of a SMART learning environment for the upskilling of cybersecurity professionals in Mauritius. *Education and Information Technologies*, *26*(2021):3175-3201. https://doi.org/10.1007/s10639-020-10408-9

Tadesse, S., & Muluye, W. (2020). The impact of COVID-19 pandemic on education system in developing countries: a review. *Open Journal of Social Sciences*, *8*(10):159. https://doi.org/10.4236/jss.2020.810011

Tajfel, H., & Turner, J.C. (2004). The social identity theory of intergroup behavior. In: J.T. Jost & J. Sidanius (eds.), *Political psychology: Key readings* (pp: 276–293). London: Psychology Press. https://psycnet.apa.org/doi/10.4324/9780203505984-16

Thomas, G., & Sule, M.J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(1):18-40. https://doi.org/10.1108/OCJ-09-2021-0025

Tolbert, M. (2021). *Vulnerabilities of multi-factor authentication in modern computer networks.* Worcester, UK: Worcester Polytechnic Institute. Available from: https://digital.wpi.edu/pdfviewer/2r36v157c

Ubaid, A.M. (2023). The critical success factors of the highly competitive organizations; a systematic literature review. *The TQM Journal, 36*(4)1020-1053. https://doi.org/10.1108/TQM-11-2022-0333

Ulker-Demirel, E., & Ciftci, G. (2020). A systematic literature review of the theory of planned behavior in tourism, leisure and hospitality management research. *Journal of Hospitality and Tourism Management*, *43*(2020):209-219. https://doi.org/10.1016/j.jhtm.2020.04.003

Utami, I., Astiti, Y.W., & Mohamed, N. (2019). Fraud intention and Machiavellianism: An experimental study of fraud triangle. *International Journal of Financial Research*, *10*(5):269-279. http://dx.doi.org/10.5430/ijfr.v10n5p269

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice*, *6*(5):100-110. https://doi.org/10.5430/jnep.v6n5p100

van der Kleij, R., Schraagen, J.M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & Security*, *113*(2022):102535. https://doi.org/10.1016/j.cose.2021.102535

Vavatsioulas, D. (2023). *Analyzing and mitigating the financial impact of cyberattacks on businesses through clustering*. Unpublished Master's thesis, University of Macedonia.

Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3):425-478. https://doi.org/10.2307/30036540

Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability management models using a common vulnerability scoring system. *Applied Sciences*, *11*(18):8735. https://doi.org/10.3390/app11188735

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*(2021):11895-11910. https://doi.org/10.1109/ACCESS.2021.3051633

Wu, T., Tien, K.Y., Hsu, W.C., & Wen, F.H. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. *Applied Sciences*, *11*(19):9266. https://doi.org/10.3390/app11199266

Xu, R., Cui, B., Duan, X., Zhang, P., Zhou, X., & Yuan, Q. (2020). Saliva: Potential diagnostic value and transmission of 2019-nCoV. *International Journal of Oral Science*, *12*(1):11. https://doi.org/10.1038/s41368-020-0080-z

Yadav, R. (2021). Cyber security threats during COVID-19 pandemic. *International Transaction Journal of Engineering Management & Applied Sciences & Technologies*, *12*(3):1-7. https://doi.org/10.14456/ITJEMAST.2021.59

Zegeye, A., Worku, A., Tefera, D., Getu, M., & Sileshi, Y. (2009). *Introduction to research methods.* Graduate studies and research office Addis Ababa University. Available from: https://uogqueensmcf.com/wp-content/uploads/2020/BA%20Modules/Psychology/Psychology%20Courses%27%20Teaching%20Materials/Second%20Year/First%20Semester/Research%20Methods%20in%20Psychology/Research%20Methods%20in%20Psychology.pdf

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

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, *8*(4):422-435. https://doi.org/10.1016/j.dcan.2021.07.006

Zomer, T., Neely, A., Sacks, R., & Parlikad, A. (2021). Exploring the influence of socio-historical constructs on BIM implementation: an activity theory perspective. *Construction Management and Economics, 39*(1):1-20. https://doi.org/10.1080/01446193.2020.1792522

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H.N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

Appendix A: Interview questions

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

Interview Schedule

At the start of each semi-structured interview, the following interview protocol points from Saunders et al. (2009) will be discussed.

a. The researcher will greet participants and express gratitude for considering the request for access and consenting to the meeting (p. 332).

b. Participants will be reminded of their right to confidentiality and anonymity and assured of it. Without first seeking and gaining the participant's express consent, the contents of the interview will not be disclosed at any time.

c. The participant will be reminded of their freedom to refuse to answer any question and to terminate the interview at any moment (p. 332).

d. Upon request, the participant will be explained how the data obtained will be used, for what objectives it will be used, and what will happen to it when the research project is over.

e. A request to record the interview electronically will be reaffirmed, even if the question would have been posed in the first invitation extended to the participant by email or hand-delivered.

f. The researcher will summarize the topics to be addressed, check the amount of time remaining, and ask the participant to read and sign the informed consent form at this point (p. 332).

What to say before the interview:
"Please feel free to refuse any question or to terminate the interview at any time. The transcripts from the recording will be used for the findings section of my study, and any names, including your name and the organization's name, and any confidential information will be blurred out and kept anonymous. Please keep in mind that when answering the questions, it should be within the scenario of an organization and the context of COVID-19 and South Africa, focusing on the cybersecurity readiness of organizations during the crisis with emphasis on employees' feelings, thoughts, perspective, and individuality."

Interview Questions
Since the interview is semi-structured, the following interview questions may be asked in any order during the actual interview, even if they are listed in numerical order. Some questions may be rephrased or eliminated entirely, while others may be added.

It is expected that the interview would run for 35 minutes. The researcher will try to set out 5 minutes before and after each interview to explain the research scenario and to close the conversation.

Research Aim	**Focused Questions to Achieve Aim**	**Time Allocation (minutes)**
Introduction	Interview Protocol Steps	5
As a cybersecurity professional, what technical implications does COVID-19 have?	- How has COVID-19 affected the technical aspect of work from your experience?	5
	- Which technical processes and system vulnerabilities were exploited by COVID that needed protection?	
	- Did COVID-19 directly impact the organization or did the digitization caused by COVID indirectly create the impact?	
As a cybersecurity professional, which cyberthreats are visible during COVID-19?	- What common cybersecurity threats have gained importance during the pandemic?	10
	- Which COVID-19 related cybersecurity attacks have occurred in the organization and how were they identified?	
	- How has COVID-19 related cyber threats changed the security landscape for you?	
	- Were there any technical vulnerabilities exploited by COVID that threatened the organization's cybersecurity?	

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

Research Aim	**Focused Questions to Achieve Aim**	**Time Allocation (minutes)**
As a cybersecurity professional, how do you mitigate pandemic-related cyberattacks?	- Which people, processes, and tools are involved in containing, mitigating, and restoring the impacts of COVID-19 risks?	10
	- How do you promote a safer cyberspace within the organization post COVID-19?	
	- How do you implement appropriate safeguards to ensure the protection of the organization's assets and processes?	
	- Which onsite and remote cybersecurity policies do you adhere to during COVID-19?	
Conclude	- What makes a South African-based organization more appealing to cyber security threats compared to operating in another country?	5
	- What is your prediction for the future of cybersecurity in South Africa post-COVID-19?	

Appendix B: Ethics approval letter

Faculty of Commerce

Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Internet: www.uct.ac.za
@Commerce UCT **UCT Commerce Faculty Office**

02 06 2022

Mahima Daya

Department of Information Systems

University of Cape Town

REF: REC 2022/06/002

Impact of COVID-19 on Cybersecurity in Organisations

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 31-Dec-2023 .

Your clearance may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility of the principal investigator.

We wish you well for your research.

Signed by candidate

2022.06.02
14:13:38 +02'00'

Jacques Rousseau
Commerce Research Ethics Chair
University of Cape Town
Commerce Faculty Office
Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375
Office Fax: +27 (0)21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Website: http://www.commerce.uct.ac.za/com/Ethics-in-Research

Appendix C: Editing certificate (Before & After Examination)

Mike Leisegang
Freelance Copy-Editor and Proofreader

Phone: +27 82 857 8733
Email: mike@wellspotted.ink
Web: www.wellspotted.ink

WELL SPOTTED

Certificate of Editing

This serves to confirm that copy-editing and proofreading services were rendered to Mahima Daya for "Analysis of COVID-19 Effects on Cybersecurity in South African-based Organisations" with a final editable page count of 130 from 3rd May 2024 to 24th May 2024

I am a member of the Professional Editors' Guild (member number LEI004) and commit to the following codes of practice (among others):

- *I have completed the work independently and did not sub-contract it out*
- *I kept to the agreed deadlines and/or communicated changes within reasonable time frames*
- *I treated all work as confidential and maintained objectivity in editing*
- *I did not accept work that could be considered unlawful, dishonest, or contrary to public interest*

I uphold the following editing standards:

- *proofreading for mechanical errors such as spelling, punctuation, grammar*
- *copy-editing that includes commenting on, but not correcting, structure, organisation and logical flow of content, basic formatting (headings, page numbers), eliminating unnecessary repetition*
- *checking citation style is correct, punctuating as needed and flagging missing or incorrect references*
- *commenting on suspected plagiarism and missing sources*
- *returning the document with track changes for the author to accept*

I confirm that I have met the above standards of editing and professional ethical practice. The content of the work edited remains that of the student.

Signed by candidate

Michael John Leisegang

Certificate in Freelance and In-house Copy-editing and Proofreading

Mike Leisegang
Freelance Copy-Editor and Proofreader

Phone: +27 82 857 8733
Email: mike@wellspotted.ink
Web: www.wellspotted.ink

WELL SPOTTED

Certificate of Editing

This serves to confirm that copy-editing and proofreading services were rendered to Mahima Daya for "Analysis of COVID-19 Effects on Cybersecurity in South African-based Organisations" with a final editable page count of 101 and 259 references from 18th November 2024 to 22nd November 2024

I am a member of the Professional Editors' Guild (member number LEI004) and commit to the following codes of practice (amongst others):

- *I have completed the work independently and did not sub-contract it out*
- *I kept to the agreed deadlines and/or communicated changes within reasonable time frames*
- *I treated all work as confidential and maintained objectivity in editing*
- *I did not accept work that could be considered unlawful, dishonest, or contrary to public interest*

I uphold the following editing standards:

- *proofreading for mechanical errors such as spelling, punctuation, grammar*
- *copy-editing that includes commenting on, but not correcting: structure, organisation and logical flow of content, basic formatting (headings, page numbers), eliminating unnecessary repetition*
- *checking citation style is correct, punctuating as needed and flagging missing or incorrect references*
- *commenting on suspected plagiarism and missing sources*
- *returning the document with track changes for the author to accept*

I confirm that I have met the above standards of editing and professional ethical practice. The content of the work edited remains that of the student.

Signed by candidate

Michael John Leisegang

Certificate in Freelance and In-house Copy-editing and Proofreading

Note: I am not accountable for any changes made to the above document by the author or any other party subsequent to my edit.

Unit 48, Amber Valley, Private Bag X30, Howick, 3290
Cell: 082 857 8733 mike@wellspotted.ink