

https://dspace.org/

The role of remote working on cybersecurity behaviour of South African financial services employees

Mabiala, Makunia Job

2020
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/41257

Mabiala, Makunia Job . (2020). The role of remote working on cybersecurity behaviour of South African financial services employees [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace.

Downloaded from a DSpace repository. https://dspace.org/

THE ROLE OF REMOTE WORKING ON CYBERSECURITY BEHAVIOUR OF SOUTH AFRICAN FINANCIAL SERVICES EMPLOYEES

Makunia Job Mabiala

2400426

2400426@students.wits.ac.za

Supervised by

Dr Kiru Pillay

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2020

ABSTRACT

Organisations put in place security policies and controls to enforce behaviours aimed at protecting computer information systems. However, these policies are put in place often ignore the context in which the behaviour occurs. Against the backdrop of Covid-19, organisations have had to abruptly adopt remote working as the new normal which presents a myriad of challenges. The purpose of this mixed-method study was to understand whether cybersecurity behaviours of employees are carried over to the remote workplace and why. Data from eight interviews with cybersecurity professionals and sixty-three questionnaires from end-users were used to answer the research question. Results showed that complaint cybersecurity behaviours were carried to the remote workplace, however, some behaviours were not always performed in the remote workplace because they impacted employee productivity. Results showed that personal attitude and sense of control had the strongest influence on employee behaviour than social influence and organisational factors. This study is important for organisations, which had to quickly adopt comprehensive remote work arrangements, by providing insights into the risks posed by remote working, formulating response strategies to reduce these risks and developing strategies that make their employees the first line in terms of protecting them against threats to cyber security.

KEYWORDS

Cybersecurity Behaviour, Information Security, Policy compliance, Computer security; Remote Working, Financial Services, South Africa

DECLARATION

I, **Makunia Job Mabiala**, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Makunia Job Mabiala

X

Makunia Job
Student

Signature:

Signed at: **Sea Point, Cape Town**

On the **30** …….. day of **June** 2020

DEDICATION

This is dedicated to my wife Vanessa Kogere Mabiala who along with other frontline workers have put their lives on the frontline to combat the COVID-19 pandemic, sometimes at the cost of their health. I salute you all.

ACKNOWLEDGEMENTS

I would like to acknowledge Dr Kiru Pillay, my supervisor, who journeyed with me. You were patient with me given that this was new territory and guided my thought process. Thank you for being a source of support and continuous encouragement. I would also like to thank my company Viadex, with special mention to Manda Doveton and Brian Dunleavy, for supporting me on this journey. A special acknowledgement goes to my family, Amen Christian Church Community and friends for the support.

TABLE OF CONTENTS

ABSTRACT ..... **ii**

DECLARATION ..... **iv**

DEDICATION ..... **v**

LIST OF TABLES ..... **xi**

LIST OF FIGURES ..... **xii**

LIST OF ACRONYMS ..... **xiv**

CHAPTER 1. INTRODUCTION **1**

1.1 PURPOSE OF THE STUDY 1
1.2 CONTEXT OF THE STUDY 1
1.3 RESEARCH PROBLEM 4
1.4 RESEARCH QUESTIONS 5
1.4.1 WHAT CYBERSECURITY BEHAVIOURS DO COMPANIES EMBED ON EMPLOYEES THROUGH AWARENESS AND TRAINING WHEN WORKING WITHIN THEIR PREMISES? 5
1.4.2 TO WHAT EXTENT ARE CYBERSECURITY BEHAVIOURS EMBEDDED IN A PHYSICAL WORK LOCATION RETAINED IN REMOTE WORKING? 5
1.4.3 WHAT FACTORS INFLUENCE CYBERSECURITY BEHAVIOURS WHEN EMPLOYEES WORK REMOTELY? 5
1.5 SIGNIFICANCE OF THE STUDY 5
1.6 DELIMITATIONS OF THE STUDY 7
1.7 DEFINITION OF TERMS 7
1.8 ASSUMPTIONS 8
1.9 CHAPTER OUTLINE 8

CHAPTER 2. LITERATURE REVIEW **9**

2.1 INTRODUCTION 9
2.1.1 DEFINITION OF CYBERSECURITY 10
2.1.1 CYBERSECURITY POSES A CHALLENGE 11
2.1.2 THE ROLE OF PEOPLE IN CYBERSECURITY 12
2.1.1 PEOPLE ARE THE WEAKEST LINK 13
2.1.2 THE IMPACT OF SOCIAL SETTING 15
2.1.3 WHAT BEHAVIOURS ARE ENFORCED IN THE OFFICE ENVIRONMENT 15
2.1.4 CYBERSECURITY BEHAVIOUR THEMES 19
2.1.1 THE ROLE OF POLICIES ON CYBERSECURITY BEHAVIOUR 20
2.1.1 THE ROLE OF TRAINING ON DRIVING CYBERSECURITY BEHAVIOUR 21
2.1.2 NEED FOR MIXED-METHOD STUDIES 21
2.1.3 THE SOUTH AFRICAN FINANCIAL SERVICES INDUSTRY 22

2.1.4 Proposition 1 23
2.2 Which cybersecurity behaviours are carried to the remote work environment 23
2.2.1 Definition Of Remote Working 23
2.2.2 Remote working influences overall employee behaviour 24
2.2.3 Remote working and security behaviours 25
2.2.4 Proposition 2 26
2.3 Which cybersecurity behaviours are carried to the remote work environment 26
2.3.1 Defining cybersecurity behaviour 26
2.3.2 What influences cybersecurity behaviour 27
2.3.3 Hypothesis 29
2.4 Conclusion of Literature Review 29
2.4.1 Proposition 1 29
2.4.2 Proposition 2 29
2.4.1 Hypothesis 1 29
2.5 ANALYTICAL FRAMEWORK 30
2.5.1 Theoretical Framework 30
2.5.2 Conceptual Framework 31

CHAPTER 3. RESEARCH METHODOLOGY 33

3.1 Research approach 33
3.2 Research design 35
3.3 Data collection methods 37
3.4 Population and sample 38
3.4.1 Population 38
3.4.2 Sample and sampling method 39
3.5 The research instrument 43
3.6 Procedure for data collection 44
3.7 Data analysis and interpretation 46
3.7.2 Definitions of variables 49
3.7.3 Data analysis procedure 50
3.7.4 Methods of data analysis 51
3.8 Limitations of the study 51
3.9 Validity and reliability/transferability and dependability 52
3.9.1 Transferability 52
3.9.2 Credibility 52
3.9.3 Reliability and dependability 52
3.10 Demographic profile of respondents 53
3.11 Ethical considerations 54

CHAPTER 4. PRESENTATION OF FINDINGS AND RESULTS . 58

Introduction 58
Table 2: How results fit into the Consistency Matrix 59
4.1 Results pertaining to Proposition 1 61
4.1.1 Password Management 63
4.1.2 Information Handling 64

4.1.3 Email Use 64
4.1.4 Mobile computing 65
4.1.5 Social networking sites (SNS) use 65
4.1.6 Incident reporting 66
4.1.7 Internet use 66
4.2 Results pertaining to Proposition 2 67
Table 4: Summary of cybersecurity behaviours carried to the remote work environment 69
4.3 Results pertaining to Proposition 3 70
Descriptive Analysis of the Study Variables 70
4.3.1 Intent 70
4.3.2 Personal Attitude Scale 71
4.3.3 Social Influence 73
4.3.4 Sense of control 75
4.3.5 Organisational Factors 77
4.4 Summary of the results/findings 79

CHAPTER 5. DISCUSSION OF THE RESULTS OR FINDINGS . 80

Introduction 80
5.1 Discussion pertaining to Proposition 1 80
5.2 Discussions pertaining to Proposition 2 82
5.3 Discussion pertaining to Hypothesis 1 85
5.3.1 Intent 85
5.3.2 Personal Attitude 85
5.3.3 Social influence Scale 87
5.3.4 Sense of Control Scale 89
5.3.5 Organisation Measures 90
5.4 Conclusion 92

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS 93

6.1 Introduction 93
6.2 Conclusions regarding research objective 1 93
6.3 Conclusions regarding research objective 2 94
6.4 Conclusions regarding research objective 3 94
6.5 Recommendations 96
6.6 Suggestions for further research 96

REFERENCES.....98

APPENDIX A: Interview Request 117

APPENDIX B: Interview Protocol.....119

APPENDIX C: Summary of thematic analysis 121

APPENDIX D: Instrument – Questionnaire 122

APPENDIX E: Financial Services LinkedIn Group 127

LIST OF TABLES

Table 1: Consistency Matrix 57

Table 2: consistency Matrix in relation to results 60

Table 3: Examples of codes derived from participant B about behaviours enforced in the office environment. 61

Table 4: summary of changes in cybersecurity behaviour in the remote work environment 70

Table 5: Personal Attitude Regression Analysis 73

Table 6: Social Influence Regression Analysis 75

Table 7: Sense of Control Regression Analysis 77

Table 8: Organisation Factors Regression Analysis 79

LIST OF FIGURES

Figure 1 Core aspects in cybersecurity adopted from Safa, von Solms, & Futche (2016) 1

Figure 2: Percentage of WFH Workers as a Result of the Pandemic (Oltsik, 2020) 4

Figure 3. *Two-factor taxonomy of end-user security behaviours (Adopted from Stanton et al.* 17

Figure 4:the role of policies and training on cybersecurity behaviour (Parsons et al., 2014) 21

Figure 5 categorising behaviours enforced in the workplace. Adopted from Parsons et al., 2014 (2014) 31

Figure 6 factors influencing cybersecurity behaviours. Adopted from (Ajzen & Fishbein, 1973) 32

Figure 7: Convergent mixed-method study (Fetters et al., 2013) 37

Figure 8: data collection process for quantitative data 42

Figure 9 coding process informed by Braun & Clarke (2006) 49

Figure 10 coding strategy 59

Figure 11 summary of identified behaviours in the office environment. 63

Figure 12: thematic analysis snapshot from the coding tool Quirkos 63

Figure 13: summary of behaviours enforced in the workplace 67

Figure 14: Descriptive analysis of Personal Attitude 72

Figure 15: Descriptive analysis of Social Influence 74

Figure 16: Descriptive analysis of Sense of Control 76

Figure 17: Descriptive analysis of Organisation Factors 78

LIST OF ACRONYMS

Acronym	Definition
HAIS-Q	The Human Aspects of Information Security Questionnaire
TPB	Theory Of Planned Behaviour
PC	Personal Computer
BOYD	Bring Your Own Device
ITU	International Telecommunication Union
SAB	Security Assurance Behaviour
SCB	Security Compliant Behaviour
SRB	Security Risk-taking Behaviour
SDB	Security Damaging Behaviour
IT	Information Techology
WFH	Work From Home

CHAPTER 1. INTRODUCTION

1.1 Purpose of the study

This mixed-method study will explore whether employees continue to comply with cybersecurity behaviours embedded put in place within company parameters when they work remotely.

1.2 Context of the study

As the world becomes more digital and interconnected, businesses, particularly financial services intuitions, face an array of security-related threats that negatively impact their information systems (Kirlappos, Parkin, & Sasse, 2015). Cybersecurity breaches cost South African ZAR50 billion and are expected to continue rising (Von Solms & Van Niekerk, 2013), with financial institutions being a primary target. Threats such as ransomware, unauthorised payments, disruption of online systems and theft of client data can inflict financial and reputational damage (Deloitte, 2019). To minimise such threats, businesses invest in technologies that protect their information systems, mainly consisting of unified threat management, firewalls, endpoint software and intrusion detection.

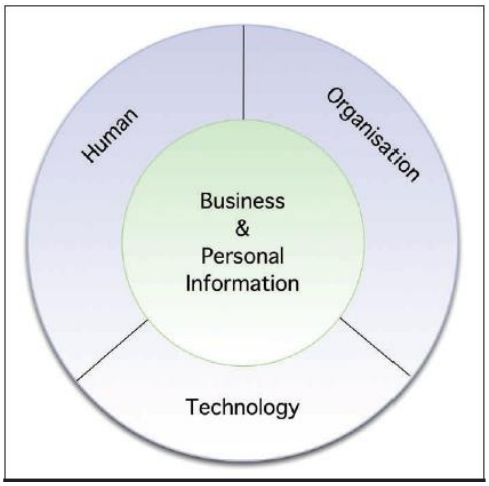


Figure 1 Core aspects in cybersecurity adopted from Safa, von Solms, & Futche (2016)

Figure 1 illustrates critical elements in protecting information (Safa et al., 2016), it is evident that information is an asset that requires human, organisational, and technological efforts to effectively protect it.

Researchers have argued that technology controls alone are insufficient and that people are critical to cybersecurity (Adams & Sasse, 1999; Pfleeger, Sasse, & Furnham, 2014; Sasse, Brostoff, & Weirich, 2001; Sohrabi Safa et al., 2016).

Researchers have given significant attention to the human aspect in cybersecurity (Pfleeger, Sasse, & Furnham, 2014) by focusing on understanding and predicting behaviours that drive the human error in cybersecurity behaviours to help organisations better mitigate these costly errors. For example, Stanton et al. (2005) introduced categories of cybersecurity behaviours, Leach (2003) focused on what influences cybersecurity behaviour and Safa et.al. (2016) focused on how personality traits influence cybersecurity behaviour. Research shows that when employees are aware of the risks associated with mishandling of information at their disposal, their behaviour in the organisation plays a significant role in mitigating risk (Stephanou & Dagada, 2014).

Increasingly, organisations and people are having to adjust to a new way of working. The employee is no longer bound to carrying out daily activities within company parameters (Gajendran & Harrison, 2007), leading to a phenomenon referred to as remote working. This has forced organisations to grant access to protected resources from external access points that are at times controlled by different hosts – for example, an employee's internet service provider or the coffee shop internet service provider – which increases the risk to company's internal resources (Souppaya & Scarfone, 2016). When employees work remotely, it creates more concerns such as lack of physical security controls, use of unsecured networks and exposure of internal resources to external parties (Furnell & Shah, 2020). Cybersecurity policies and controls put in place by organisations presume that the employees will make use of computer information systems within the company parameters – for example, the head office or branch office and often ignore the context where these behaviours take place (Da Veiga & Eloff, 2010; Alotaibi, Clarke, & Furnell, 2020; Chen, Ramamurthy, & Wen, 2012). This is not always the case, as researchers have found that employees

don't always adhere to cybersecurity-related behaviours, even when working within company bounds (Safa et al., 2015).

There is however limited research on employee cybersecurity behaviour in the remote workplace - many studies ignore or pay little attention to the context in which cybersecurity behaviour occurs - e.g. working from home or coffee shop. Kirlappos et al. (2015) found a link between the context (physical location of the end-user) and the behaviour. In their study, employees were aware that they need to lock their screens and how to do so but it did not do because – in their specific work context – they felt it would display a lack of trust in their work colleagues. Therefore, their work context was the real cause of that behaviour. When employees work remotely, they no longer have the presence of IT staff monitoring how they behave, this leads to negligent behaviours or naïve mistakes (Souppaya & Scarfone, 2016).

This requires further discussion and research because humans adapt their behaviour to the environment, sometimes ignoring some intrinsic factors like moral code (ENISA, 2019). Understanding the underlying cause of cybersecurity behaviour, businesses can put in place effective measures (more education) to reduce the threat of cybersecurity. Covid-19 has impacted the way we work, resulting in a growing population of Work From Home (see Figure 2) employees – with the majority of companies supporting between 91 per cent and 100 per cent WFH employees (Oltsik, 2020). While technology-enabled businesses continue operating, it also presents a myriad of challenges – for example, users taking shortcuts and ignoring procedures because there was not the physical presence of IT staff (Tessian, 2020). It is important to understand the role that remote working has on cybersecurity behaviours.

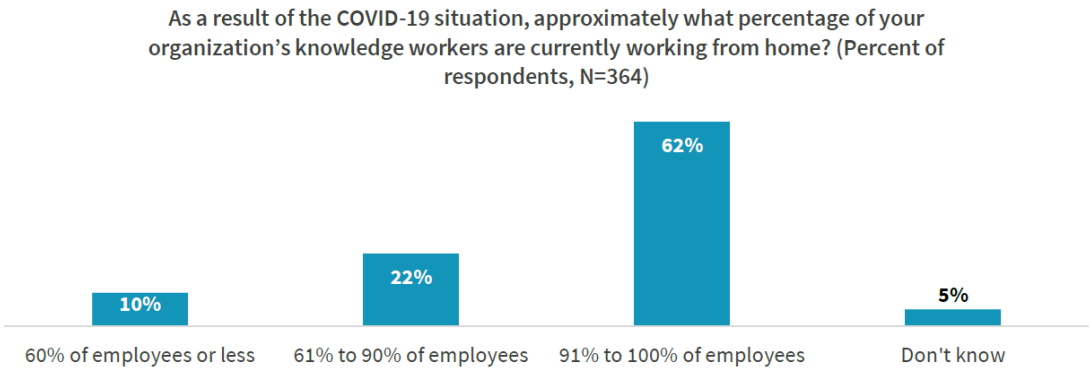


Figure 2: Percentage of WFH Workers as a Result of the Pandemic (Oltsik, 2020, p. 17)

1.3 Research Problem

Organisations rely on computer information systems for daily operations and have put in place measures to protect their function. While technological mechanisms such as firewalls provide protection, the behaviours of employees towards computer information systems play a pivotal role in their implementation and usage. Consequently, organisations put in place security policies and controls to enforce behaviours aimed at protecting computer information systems. However, these policies are put in place to drive behaviour within the organisation's parameters with little attention given to remote working (Furnell & Shah, 2020). Even within company bounds, enforced behaviours do not manifest as employees take corners or ignore rules set out in cybersecurity policies. Against the backdrop of Covid-19, organisations have had to abruptly adopt remote working as the new normal which presents a myriad of challenges. One example is that within work parameters IT administrators monitor and enforce security behaviour, but this control is lost when employees work remotely (Furnell & Shah, 2020). Another is that employees working remotely are used as a primary target to infiltrate organisation systems. Therefore, securing computer systems will rely on employees retaining learned behaviour within organisation parameters when working remotely (Malecki, 2020). It is therefore important to understand the role of remote working on learned cybersecurity behaviours in order to determine whether cybersecurity behaviours learned within company parameters transfer to the remote working environment.

1.4 Research questions

To understand the role of remote working, we need to understand the underlying changes – for example, what behaviours are entrenched when employees work within company parameters, how are they influenced when they work remotely. Therefore, the research question as follows

- **1.4.1** ***What cybersecurity behaviours do companies embed on employees through awareness and training when working within their premises?***
- **1.4.2** ***To what extent are cybersecurity behaviours embedded in a physical work location retained in remote working?***
- **1.4.3** ***What factors influence cybersecurity behaviours when employees work remotely?***

The first question explores the current state of cybersecurity behaviours companies aim to embed in their employees in order to reduce cybersecurity risk. The objective of the first question is to provide an overview of standard security practice form the human aspect of cybersecurity within the financial services industry. The second research questions aims to uncover which of the cybersecurity behaviours uncovered in the first question are carried over to the remote work environment. The researcher acknowledges that the first two questions will be better unset by cybersecurity professionals who have an overarching view of organisational security posture.

The third research question aims to understand what influences the change or no change in cybersecurity behaviour when employees work remotely. This question benefits from the responses of employees, also refer to as end-users in this research. For these questions, the study takes into consideration the null hypothesis by testing for the alternative hypothesis.

1.5 Significance of the study

This study is important for organisations, which had to quickly adopt comprehensive remote work arrangements, by providing insights into the risks

posed by remote working, formulating response strategies to reduce these risks and developing strategies that make their employees the first line in terms of protecting them against cybersecurity threats. There is a growing belief that to protect information technology resources from cybersecurity threats, the people driving the measures need to be part of the solution and not the problem (Aminzade, 2018; Safa, von Solms, & Futcher, 2016; Safa, Von Solms, & Furnell, 2016). This has led to a growing library of academic research seeking to address the role of people in cybersecurity by focusing on understanding, predicting and changing. Many studies ignore the context in which cybersecurity behaviours occur – such as the environment of work and how that affects behaviour.

Previous research considering work environment primarily focused on the understanding behaviour within the physical work environment – company offices (Cheung, Chang, & Vincent, 2000; Ayyagari, Grover, & Purvis, 2011; Ament & Haag, 2016). Cheung et al. (2000) argued that facilitating conditions (e.g. geographic and resource limitations) and social factors are fundamental drivers of behaviour. Ayyagari et al. (2011) found a link between work-related stress and role uncertainty to be drivers of behaviours. Ament & Haag (2016) studied the role of an individuals' work, personal, and social environment and the study found mixed results but pointed to the behaviour being influenced.

In the case of Ament and Haag (2016), which focused on work, personal, social environments physically separate, further research will be needed because the three elements will be in one physical location. Ensuring that remote working employees have the necessary cybersecurity is a challenge for businesses globally (Oltsik, 2020), assessing how it influences behaviour will be a valuable contribution to the cybersecurity debate. This study will contribute to the ongoing search for understanding what drives cybersecurity behaviour. Remote working will become the new norm, companies will have to amend policies and ultimately the behaviours they enforce. For this, they will need a better understanding of the employee experience with cybersecurity policies when working remotely. From a South African perspective, it will help businesses understand behaviours that are unique to our society. Our societal landscape differs from that of the United States of America and Europe as well as Asia, where most studies are conducted. This

research will provide insights that will benefit future studies and businesses, especially those within South Africa or looking to operate in the country.

1.6 Delimitations of the study

Remote working may have already been in place for some companies prior to the Covid-19 pandemic (Okereafor & Manny, 2020), this study focuses on a particularly intense period of remote working. Therefore, this study focuses on South African landscape that were forced to implement mass remote working during due to the Covid-19 pandemic. This focuses on the South African financial services sector only. The decision was driven by notion that financial services companies are follow regulated guidelines and are required to have mature cybersecurity systems and procedures in place (Deloitte, 2019).

1.7 Definition of terms

- Cybersecurity behaviour: actions of end-users when interacting with cybersecurity system (Von Solms & Van Niekerk, 2013)
- Context: The place (physical setting) where cybersecurity behaviour occurs (ENISA, 2019)
- Remote working: any arrangement where the employee works from a location that is outside the company physical environment or client site to carry out job-specific related tasks (Felstead & Henseke, 2017)
- Naïve Mistakes: negative cybersecurity behaviour by an employee with no intention to expose the organisation to cybersecurity threats (Stanton, Stam, Mastrangelo, & Jolton, 2005)
- Basic hygiene: positive cybersecurity behaviour by an employee with the intention to protect the organisation against cybersecurity threats (Stanton et al., 2005)
- Compliant Behaviour: cybersecurity behaviours that are in line with company policies and procedures. Compliant behaviour in the human

element of cybersecurity is cybersecurity behaviour that is meets the definition of basic hygiene (Guo, 2013).

- Risky Behaviour: any behaviour in line with naïve mistake (Gangire, Da Veiga, & Herselman, 2020)

1.8 Assumptions

The research assumes that human cybersecurity behaviour is influenced by their work environment and that outside the organisational parameters where certain rules are in place to drive positive behaviour – which may be neglected when working remotely. The study also assumes that no other work factors – hours, job function, reporting structure – have changed except for the physical location of the end-user.

1.9 Chapter Outline

This chapter introduced the cybersecurity challenge – cybersecurity breaches – faced by businesses globally and in Africa. The chapter highlighted South Africa's unique landscape and the impact of Covid-19 on the way we work. The chapter highlighted the need for this research and why it is worth pursuing. The next will explore literature to provide a comprehensive summary of previous research on the topic.

CHAPTER 2. LITERATURE REVIEW

2.1 Introduction

The purpose of this chapter is to provide a background to the themes that lead to the problem statement. This chapter will present the arguments identified on this topic by discussing and analyzing existing literature on this subject matter. Specifically, this chapter will also serve the purpose of highlighting the shortcomings of existing literature on the matter of cybersecurity behaviour of remote workers and the need for further research to build on the body of knowledge. Researchers have also called for further investigation into the role of the context (for example, the office environment) in which cybersecurity behaviour (for example, browsing social media sites) occurs. Therefore, this chapter will point the need for further research as a request by other authors.

This literature review is not driven by the purpose of summarizing all literature published on cybersecurity behaviour but show areas that the researcher has identified patterns or themes, common practices, and gaps in the existing literature. The literature review was conducted by researching reputable cybersecurity, information security and information technology academic journals. Given that this research also borrows from the field of psychology, research focused on human behaviour were also consulted. The researcher used personal relationships with a partner company CybSafe, a cybersecurity training company based in the United Kingdom with a reputable database of the cybersecurity-related academic database. Academic database journal databases such as Science Direct, Emerald, JSTOR and Springer were used to find relevant publications. The University of Witwatersrand's electronic library served as a gateway to access gated journals. Google Scholar was also explored for more complex keyword searchers given Googles proclaimed algorithms that rank well-cited articles – leading to greater credibility (Beel & Gipp, 2009).

Before continuing with this chapter, it is important to highlight the purpose of a literature review, its categories, methods and the steps taken for this study. The

purpose of a literature review is to provide the researcher with the opportunity to demonstrate how their research integrates with the larger body of knowledge in the field of study (Okoli & Schabram, 2010). The literature review assists the researcher in achieving this by providing a summary of sources explored in investigating the problem (Onwuegbuzie, Leech, & Collins, 2015). Reviewing literature plays another vital function that looks beyond simply summarizing sources explored. In the field of social sciences, for example, a literature review follows a specific pattern that embeds both summary and synthesis within existing conceptual categories (Okoli & Schabram, 2010).

2.1.1 *Definition of cybersecurity*

Before delving into people's roles in cybersecurity, it is important to define what is cybersecurity. It is well documented that there is no standard definition of cybersecurity, with various authors and publications giving their version of the definition (Craigen, Diakun-Thibault, & Purse, 2014). This absence of a generally accepted definition leads to disagreement on the function of cybersecurity, what is protected, from whom it is protecting, and how it is protected (Deibert & Rohozinski, 2010). The lack of a clear and widely accepted definition of cybersecurity is attributed to its multidimensional characteristics with many definitions focusing on the technical aspect of cybersecurity (Craigen et al., 2014). Even countries with well-defined and established cybersecurity strategies like the United States of America and the United Kingdom have failed to establish a definition of what cybersecurity is and is not (Von Solms & Van Niekerk, 2013).

Often confused with information security, cybersecurity is defined as *"measures taken to protect a computer or computer system against unauthorized access or attack"* by Merriam Webster. Other sources define cybersecurity as *"the process of protecting information by preventing, detecting, and responding to attacks"*. These definitions bear similarities to the definition of information security. Information security focuses on the protection of information by preserving "the confidentiality, integrity and availability" of that information (The National Institute of Standards and Technology, 2020).

For this study, the chosen definition of cybersecurity is taken from The International Telecommunication Union (ITU) as "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"*(The International Telecommunication Union, 2009, p. 2). Technology plays a significant function in supporting cybersecurity but requires users and the organization assets that "*include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment"* (The International Telecommunication Union, 2009, p. 2). This is further expanded by arguing that "*Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment"* (The International Telecommunication Union, 2009, p. 3). This is not done in a vacuum and requires organisational structures, governments, social and other human aspects working in conjunction with technology to support cybersecurity (Goodall, Lutters, & Komlodi, 2009; Schatz, Bashroush, & Wall, 2017; Zakaria, 2006).

2.1.1 *Cybersecurity poses a challenge*

Despite measures put in place, cybersecurity is a major challenge for businesses, governments and society at large (Reddy & Reddy, 2014). Emergent technologies that have redefined daily lives positively have also created scenarios where safeguarding valuable information and its systems have become nearly impossible (Jang-Jaccard & Nepal, 2014). This is because cyber crimes are easier to execute and tracking the perpetrator. Cybercrime is a term to define any illicit activity executed using a computer (Reddy & Reddy, 2014). A PwC report found that 26 % of businesses in South Africa anticipated cybersecurity-related attacks to be the primary economic crime by the year 2020 (PwC, 2020). In examining the financial impact of cybersecurity IBM discovered that cybersecurity breaches cost South African companies R40 annually and the impact stretches to lost customers (IBM, 2020). Government authorities have also seen an increase in cybersecurity-related incidents and have implemented

measures to curb them (Von Solms & Van Niekerk, 2013). Cybersecurity has become topical because information has become the backbone of every business and is seen as the driver of competitive advantage (Stephanou & Dagada, 2008; Kirlappos, Sasse, & Parkin, 2015), which has led to increased dependence on computer-based information systems (Karyda, Kiountouzis, & Kokolakis, 2005). Information systems encompass the information that is captured and stored, the technology that is configured to ensure that the information serves its purpose, the organisation responsible for the data and the procedures that govern the actions of information users (Kirlappos, Sasse, & Parkin, 2015). It is therefore important to note that the functioning and protection of information requires the organization, the technology as an enabler and humans as the custodians. This paper, therefore, argues that cybersecurity attacks have ramifications that negatively impact humans and society at large (Von Solms & Van Niekerk, 2013).

2.1.2 *The role of people in cybersecurity*

People can fulfil various roles in the overall function of cybersecurity security - such as a user of information systems, custodians of information and attacker of information (Safa, Von Solms, & Furnell, 2016). The notion of the people playing important role in securing information is not a novel concept – dating as far back as far as the 1800s when cybersecurity groundwork was taking place. In formulating principles to securely manage end to end communication, Auguste Kerckhoffs (1899) presented six principles that would enable security operating communication systems. Half of these principles were significant attention on getting people to behave in a certain way. Almost a century later, Saltzer and Schroeder gave attention to the critical role of humans in cybersecurity by recommending that the securing of information in computer systems needs to be grounded on the human element in their 1975 study (Smith, 2012). They suggested that for security mechanism to be effective, humans who apply it must accept it, the effort required to breach the system must outweigh the resources of the attacker and the defence mechanisms need to create should create as little work as possible for the organisation as a whole (Smith, 2012).

Despite this philosophy, previous research in the field of cybersecurity-focused heavily on the technology that protects against attacks (Safa et al., 2015). People were merely seen as an element of cybersecurity and that their behaviour can be governed by cybersecurity policies and enforced by security mechanisms and punishment (Kirlappos et al., 2015). This is partly because it is easier to measure and control information technology systems than it is to control human behaviours (Furnell & Clarke, 2012). Equally, measuring return in investment is a simpler task for measuring technological effectiveness compared to measuring behaviour (Furnell & Clarke, 2012). This is changing however, organisations have realised that technology alone cannot secure information ('Development and validation of instruments of information security deviant behavior', 2014; Herath & Rao, 2009; Sohrabi Safa et al., 2016), it needs collaboration with the people who manage it. This gave rise to a plethora of authors focused on better understanding cybersecurity behaviour and in the process growing the field of the human aspect of cybersecurity (Schatz et al., 2017; Warkentin & Willison, 2009).

2.1.1 *People are the weakest link*

As discussed in the introduction of this literature review, humans, the organization, and technology work together seamlessly to support cybersecurity. In this triangular component of cybersecurity, people are viewed as the weakest link in the security chain (Benbasat, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; Guo, Yuan, Archer, & Connelly, 2011; Pfleeger et al., 2014; Sasse et al., 2001). Because information is vital to the operation of businesses, it is usually subject to information related threats that can be costly from a financial and business reputation point of view (Kirlappos, Parkin, & Sasse, 2014; Pfleeger et al., 2014). While threats can come from outside the organisation, the majority happen because of an error from someone inside the organisation (Wong, Tan, Tan, & Tseng, 2019). It is this phenomenon that has driven attention to the human aspect of cybersecurity, specifically the behaviours that drive these errors. This is because it takes less effort to try to break into an encrypted system – which requires more time, skills, and resources – than it is to manipulate an employee with full access (Stephanou & Dagada, 2008). In the field of the human element of cybersecurity, authors looked at underlying causes that make people the

weakest link (Bauer, Bernroider, & Chudzikowski, 2017; Spitzmüller & Stanton, 2006). Many have paid specific attention to the fact that security mechanisms are not always successful. Researchers have highlighted the complexity that comes with trying to measure and control behaviour (ENISA, 2019).

Whitten and Tygar (1999) conducted research and uncovered that even employees who are committed to their job and adequately skilled could not use email encryption effectively - behaviour set out as a defence mechanism to protect the information. Adams and Sasse (1991) uncovered how employees did not see value in adhering to password mechanisms and policies by constantly bypassing them. These two research papers were followed by a series of research in academia that focused on demonstrating and clarifying shortcomings of security warnings (Herley, 2009) and de-risking employees by investing in cybersecurity training and education (Bada, Sasse, & Nurse, 2019; Junger, Montoya, & Overink, 2017). Arguably one of the biggest challenges that cybersecurity professionals – the people responsible for protecting the organization against cybersecurity attacks – face are getting end-users in organizations to behave safely. Therefore, research into the field of cybersecurity began borrowing from other disciplines such as psychology, economics and crime science. In summary, people are the clue that fortifies cybersecurity (Guo, 2013; Leach, 2003; Aminzade, 2018).

Schneier (2003) gave attention to the role of people in information technology systems by maintaining that for any security measure to be successful, foundational work must be carried out to get people to behave in a certain way – going back on a previous statement where he claimed that cryptography alone was the answer. Upon conducting further research into the root causes of cybersecurity incidents between 2000 and 2003 and uncovered that it takes less effort to convince trick a human than it is to hack into a computer. Hacking into a computer system requires specialized technical skills, resources, and time to decrypt sophisticated algorithms. Whilst luring a human, for example, an employee who has been given specific rights as part of their daily task fulfilment, into providing them with the required information is a simpler task. This once again stresses the importance of humans in cybersecurity.

2.1.2 *The impact of social setting*

A report conducted by ENISA (2019) highlighted that many studies on the influence of cybersecurity behaviour ignore the context in which the actual behaviour occurs. Kirlappos et al (2015) found that in addition to intrinsic factors, humans assess their behaviours about context before acting. In testing whether employees would lock their screens – as required by cybersecurity policies – workers ignored this completely even though they know how to lock their screens because a colleague stood at their desk. They felt that this would show a sense of distrust.

2.1.3 *What behaviours are enforced in the office environment*

It has been established that cybersecurity is a challenge for businesses and policymakers and the focus should be on a holistic approach – people, systems and processes to combat these challenges. It has also been established that people play an important role in reducing cybersecurity-related risk and can be the first line of defence. This next section will discuss measures put in place by organisations to make their employees the first line of defence.

Cybersecurity behaviour is defined as employee interaction with the organizations' information systems - this includes hardware, network systems, software amongst other tools - that may lead to security implications (Guo, 2013). Many approaches to identify and recognize threats have been developed. Loch et al., (1992) presented a four-dimensional approach to classify cybersecurity threats, namely (1) the origin of the behaviour, is the threat coming from inside or outside the organization? (2) perpetrators, is the threat occurring as a result of a human or non-human error? (3) The intentions, is this a deliberate action or an accident? (4) consequences, will this action lead to the destruction, altering or sharing of the information with unauthorized users? Various cybersecurity behaviours have been investigated to conceptualize the types of cybersecurity-related behaviours. Previous research has investigated computer system abuse (Straub & Nance, 1990), security breach (Workman & Gathegi, 2007), ethical use (Leonard, Cronan, & Kreie, 2004), omissive cybersecurity behaviour (Workman, Bommer, & Straub, 2008), cybersecurity policy violation (D’Arcy, Hovav, &

Galletta, 2009), non-malicious security violation (Guo et al., 2011; Ifinedo, 2019), information security policy abuse (D'Arcy et al., 2009), security policy compliance (Bulgurcu et al., 2010).

To better understand the types of cybersecurity behaviour, Stanton et al. (2015) argued every cybersecurity behaviour can be categorised into one of six categories. In his research, he asked information technology professionals and end-users to describe behaviours they would classify as favourable or unfavourable to the organization efforts to reduce cybersecurity risk. Cybersecurity professionals were then given the task of organizing these behaviours into groups without any external influences (see Figure 3). This analysis concluded that cybersecurity behaviours can be grouped into six categories, namely:

- **Intentional destruction:** any behaviour where an employee intentionally bypasses the organizations cybersecurity protocols to cause home. For example, an employee who access encrypted files on an organization's network and shares them with a competitor. This behaviour requires a high level of technical expertise to execute.
- **Detrimental misuse:** shares the same characteristics as intentional destruction bad requires minimal technical expertise. For example, using the company's email to run a side business with the company's existing customers.
- **Dangerous tinkering**: any behaviour that lacks a clear intention to bypass the organization cybersecurity protocols. For example, an employee accidentally remove passwords from the organization's Wi-Fi. To execute this behaviour the employee needs to have high technical expertise.
- **Naive mistakes:** chase the same characteristics as dangerous tinkering but with little to no technical expertise required to execute the behaviour. For example, not encrypting an email before sending it.
- **Aware assurance:** any behaviour with a strong motive to protect and idea to the organization cybersecurity protocols. For example, finding a vulnerability in one of the organization's software installed on one's PC.

- **Basic hygiene:** shares the same characteristics with away assurance but requires little to no technical expertise to execute. For example, an employee reports a phishing email to the organization's cybersecurity team.

From the description of these behaviours above, it is evident that these behaviours are observed on two levels, namely technical expertise (high or low) and intentions (malicious, neutral, or beneficial). The intention aspects capture whether the behaviour was malicious, beneficial, or somewhere in between. The technical expertise aspects capture the computer knowledge required to carry out the behaviour.

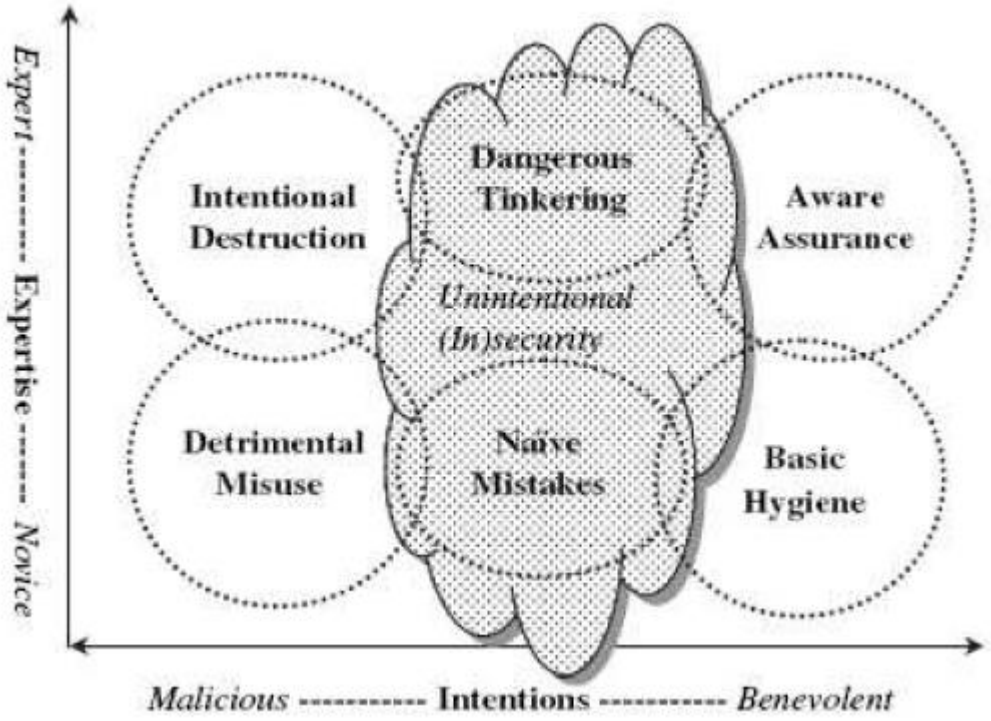


Figure 3. *Two-factor taxonomy of end-user security behaviours (Adopted from Stanton et al. 2005, p.131).*

Guo (2013) built on this work and presented four behaviour categories related to information - security assurance behaviour (SAB), security compliant behaviour (SCB), security risk-taking behaviour (SRB), and security damaging behaviour

(SDB). Security assurance behaviour (SAB) behaviour relates to the deliberate actions that employees consciously undertake to ensure that they protect the organisation against cybersecurity risk. This type of behaviour implies that an employee is not only doing what they are expected to do but going above and beyond, for example, blocking an external email address that regularly spams the organisation. This behaviour is similar to Aware assurance behaviours identified by (Stanton et al., 2005). Security compliant behaviour (SCB) applies to deliberate or accidental actions that employees take to follow cybersecurity policies.

The intent can be accidental because an employee may accidentally act in a way that violates cybersecurity policies. Security risk-taking behaviour (SRB) are behaviours that expose the organisation to cybersecurity risks a deliberate action. Although this behaviour has negative consequences, the motive may not necessarily be malicious. An employee who plugs in their flash drive to a work computer to print work-related documents may not have the intention to harm the organisation but their behaviour may increase the likelihood of harmful consequences (Guo, 2013). security damaging behaviour (SDB) applies to actions that would directly affect the cybersecurity of the company. Unlike the other mentioned behaviours like security damaging behaviour (SDB), this behaviour is intended to cause harm or damage to the organisation. This behaviour shares traits with Intentional Destruction identified by (Stanton et al., 2005). Compared to all forms of actions, this is behaviour is the most dangerous because the intent is to cause damage. Businesses focus their attention on encouraging desirable behaviour and preventing undesirable behaviour (Guo, 2013; Guo et al., 2011; Stanton et al., 2005).

In the case of Stanton et al. (2005), organisations focus their attention on driving aware assurance and basic hygiene (Chen, Ramamurthy, & Wen, 2012). Guo (2013) argue that businesses drive behaviour towards security assurance behaviour (SAB) and security compliant behaviour (SCB).

2.1.4 *Cybersecurity behaviour themes*

Parsons et al. (2014) presented a model to evaluate cybersecurity behaviours encouraged by organisations. These behaviours are driven by cybersecurity policies and training awareness programmes to reduce cybersecurity risk and built on the work by Stanton et al. (2005). The research identified key focal areas that behaviours fall in, namely password management, email use, internet use, mobile computing, Social Network use, incident reporting and information handling. They are discussed in detail below:

- **Password Management**: Addresses password behaviour by describing how users may modify their passwords using best practices for password management. It entails how to use strong and secure passwords to safeguard information system resources (Blythe, Coventry, & Little, 2015a).
- **Email Use**: The ease of forwarding emails that contain company sensitive information to personal email is one of the risks caused by employee behaviour. Email use focuses on acceptable interaction with emails that contain company information such as opening attachments in emails from unknown senders (Guo, 2013; Safa et al., 2015)
- **Mobile Computing**: focuses on how employees should access organisation information resources from outside of the company network. It usually contains a comprehensive overview of foreign mobile networks and public Wi-Fi networks, including what types of activities are permitted on such networks and if getting into work email over these networks is safe (Bauer et al., 2017; Curry, Marshall, Crossler, & Correia, 2018).
- **Internet Use**: focuses on behaviours that govern the proper usage of company employment portals and websites. With work becoming increasingly reliant on the Internet, employees can take advantage of this and start accessing dubious websites and exposing the organisation's valuable information technology assets (Bauer et al., 2017; Pattinson, Butavicius, Parsons, McCormac, & Jerram, 2015). One of the major problems that organisations face is employees downloading unauthorised software that leads to systems infiltration and malware.

- **Social Network Site**: focuses on behaviours related to the use of social network sites. Usually, social media sites can become a great source of cybersecurity risks for companies as employees may find themselves posting what seems innocent but end up costing their organisation money or reputation. Some companies place a great deal of attention and restrictions on how employees may conduct themselves online (Bauer et al., 2017).
- **Incident Report**: Cybersecurity teams are responsible for protecting a myriad of threats that they cannot track every single vulnerability (Kirlappos et al., 2015). They, therefore, rely on employees to report incidents as quickly as possible so that they can resolve them. Incident reporting is an integral part of the cybersecurity function because it turns employees into the first line of defence. This category focuses on behaviours that guide how employees can report cybersecurity-related incidences (Calic, Pattinson, Parsons, Butavicius, & McCormac, 2016).
- **Information Handling**: focuses on guiding the behaviours of employees when working with sensitive business information. organisations ensure that employees understand the nature of the information that they are working with, and how to ensure that it does not get into the wrong hands (Blythe et al., 2015a).

Researchers have highlighted that the focus areas of the Human Aspects of Information Security Questionnaire (HAIS-Q) provide a good assessment tool of cybersecurity behaviours encouraged in the workplace (Calic et al., 2016; McCormac et al., 2017; Parsons et al., 2017). It was used in this study to categorise themes found for the first proposition.

2.1.1 *The role of policies on cybersecurity behaviour*

Companies invest in cybersecurity policies that drive employee responsible conduct by providing detailed instructions on basic hygiene behaviour (Flowerday & Tuyikeze, 2016). Companies utilize this to distinguish between employee behaviour that is allowed and/or banned and resultant punishments when prohibited behaviours take place. It serves the function of safeguarding

information, systems, employees and the whole organization. It also serves as an excellent statement about the security strategy of the company to the outside world (Siponen, Adam Mahmood, & Pahnila, 2014). It also serves regulatory requirements by guiding management's efforts for the management of information safety in line with business requirements and laws (Flowerday & Tuyikeze, 2016). With the help of international standards and regulations, policies formulated are driven by company security objectives and communicated with the rest of the business (Kirlappos, Sasse, & Parkin, 2015). These policies live within the organisation intranets and clearly outline expected behaviour, the role of the employees and repercussions for non-compliance (Safa, Von Solms, & Furnell, 2016) Assessing cybersecurity policies provides a good summary of behaviours that companies expect from their employees.

2.1.1 *The role of training on driving cybersecurity behaviour*

Organisations formulate training activities focused on cybersecurity to increase employee awareness and capability. Several studies have found cybersecurity training as an integral part of influencing employee basic hygiene behaviour. D'Arcy et al. (2009) argue that when employees are aware of what is required of them, it leads to increase interest in helping the organisation reduce cybersecurity risk. Because education initiatives put in place by the organisation focus on educating, training and increasing awareness (Ifinedo, 2019), this study argues that awareness and training will positively influence basic hygiene cybersecurity behaviour.

2.1.2 *Need for mixed-method studies*

Researchers have been encouraged to use several sorts of research strategies, as there is no one means of doing research (Gable & Gable, 2016). Enisa (2019) Argue that though quantitative cybersecurity studies are often seen as the primary message of analysis and data collection, attention needs to be given to other forms of data collection such as qualitative methods. Crossler et al., (2013) stressed the necessity for research to explore ways to effectively collect, generate and measure data relating to security, especially attitude data. The lack of

methodologies that gathers deeper insights about cybersecurity behaviour presents an opportunity for this research to contribute to the body of knowledge. Enisa (2019) recommends combining quantitative and qualitative methods because current models are not well suited for behavioural research in the cybersecurity space.

2.1.3 *The South African Financial Services Industry*

The role of remote working on cybersecurity behaviour was limited to the financial services industry to increase feasibility. The financial services sector (see Figure 4) is of particular interest given how regulated they are and attractive they are to malicious attackers (Terekhova, 2018). The South African financial services sector is of the catalysts for economic growth, job creation, the construction of essential infrastructure, and long-term prosperity for South Africa and its citizens (National Treasury, 2011, p. 1). The finance sector in South Africa is responsible for 3.9 per cent of jobs and contributing at least 15 per cent of corporate income tax. It also contributes 10.5 per cent to the GDP of the economy annually due to its R6 trillion in assets (National Treasury, 2011).

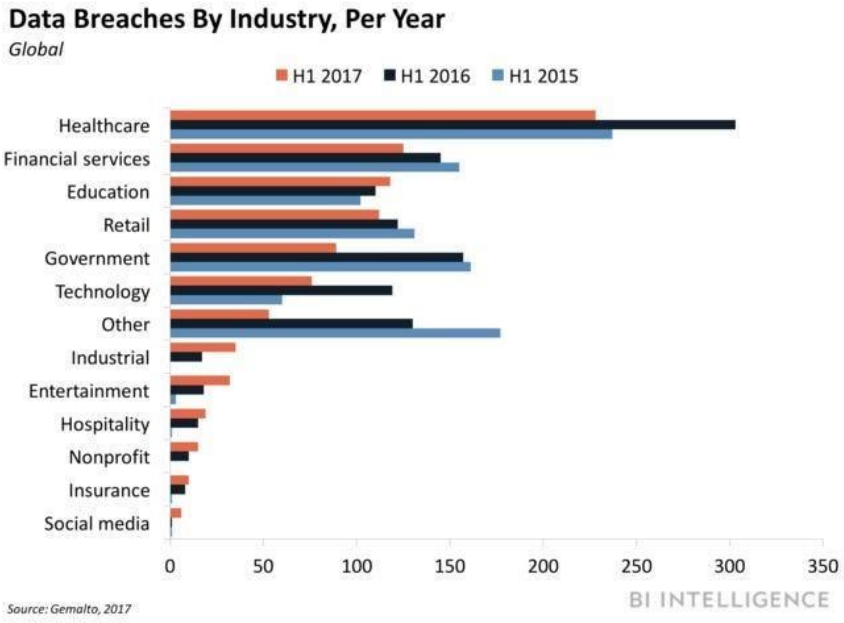


Figure 4:cybersecuirty breaches by industry (Terekhova, 2018)

2.1.4 *Proposition 1*

The first proposition posits that organisations enforce basic hygiene behaviours in the office environment.

2.2 Which cybersecurity behaviours are carried to the remote work environment

Kirlappos et al., (2014) argue that cybersecurity behaviours enforced in the office environment ignore the context in which the behaviour takes place. Having established the behaviours enforced in the workplace in the first proposition, the next step is establishing whether they are transferred to the remote working environment.

2.2.1 *Definition Of Remote Working*

Remote working refers to an arrangement where the worker does not commute or travel to a central work environment to conduct work (Smith, 2012). It mainly referred to as telecommuting in the United States of America while the rest of the world refers to it as remote working or teleworking. It is not a new concept and has been around before the invention of the world wide web. The industrial revolution brought about the need for the creation of factories and automation that required employees to be stationary where machines were to complete their work. Before this being the norm, work consisted of skilled craftsmen – such as potters, fabric makers, blacksmiths carpenters – who worked and sold their merchandise from home (We Work Remotely, 2018). Since then, paid work was not only limited to designated hours at a single venue, especially for supervisors, specialists, and other white-collar employees (Felstead & Henseke, 2017).

Advancements in technology have played a significant role in increased mobility in businesses thus the increased reliance on remote working. Technologies such as Wi-Fi, smartphones, laptops, and tablets has enabled employees to now work from just about any location (Regus, 2017). Despite remote working being around since the shift to mobile, it was not a widely adopted practice. Work From Home (WFH) is a subcategory of remote working where the employee works solely from

their home but their function, task, reporting structure and schedule stays the same. The recent changes driven by the Covid-19 pandemic has forced governments around the world to impose quarantines forcing people to be homebound. As a result, businesses around the globe had to rapidly adjust to putting in place mechanisms that enabled employees to work from home (Curran 2020). Organisations expect to support between 91 per cent and 100 per cent will function from their homes (Oltsik, 2020).

For this study, remote working is defined as “remote work is an operating model that enables the workforce to fulfil their duties away from the typical office environment” (Deloitte, 2020)

2.2.2 *Remote working influences overall employee behaviour*

Gajendran & Harrison (2007) present an intervening proposition regarding the impact of remote working on work-related aspects such as job performance. They argue that the location itself doesn’t influence behaviour and that is a psychological process or intervening mechanism to which working from home has its influence. They present 3 broad themes of these phycological processes, the first is a sense of control or autonomy that comes with working remotely followed by better managing work-life requirements and lastly, being the relationship with a colleague. These can be summarised as follows:

- Autonomy: Also known as psychological control, focuses is an integral component of work arrangements and has to do with an employee’s analysis of the control they have on how and when to complete a job-related task (Gajendran & Harrison, 2007; Daniels, Lamond, & Standen, 2000). Researchers have found that working from home increases perceived autonomy (Bliese & Edwards, 2017) which intern increase their productivity.
- Work-life balance: focuses on the balanced integration of meeting work of requirements from personal and work requirements (Gajendran & Harrison, 2007). Working from home has been seen as a driver of improved work-life balance (Beauregard & Henry, 2009).

- Relational impoverishment at work: focuses on decreased relational bonds between employees and their coworkers or their supervisors (Gajendran & Harrison, 2007). Research shows that working from home decreases interrelational bonds between employees and their coworkers or supervisors (Golden, 2006).

From the above, we deduce that remote working from increases autonomy and work-life, because of this, employees would perform at their best. This increase, however, negatively influences cybersecurity behaviour in the remote workplace (Kirlappos et al., 2015).

2.2.3 *Remote working and security behaviours*

Remote working has gained research attention given how it alters how business was traditionally operated and impacts various implications on societal matters such as commute mechanisms (Kitou & Horvath, 2006) and lifestyle balance (Gajendran & Harrison, 2007). Researchers argue that businesses benefit from having employees working remotely – such as reduced overheads and rent, (McNall, Masuda, & Nicklin, 2009). Employees also highlight benefits such as improved productivity, flexibility and improved morale as a result of remote working (Noonan & Glass, 2012; Rupietta & Beckmann, 2018). Understanding the context of the underlying behaviour is something researchers have given little attention to. Kirlappos et al. (2015) highlight that research gives much attention to understanding correlation not so much to the cause. For example, Safa et al (2016) found that experience, collaboration, cybersecurity knowledge sharing and intervention made employees adhere to organisational cybersecurity policy (behaviour). However, Kirlappos et al. (2015) found that employees knew that had to lock their screens and knew how to do it but ignored it at a particular moment because it would show distrust to a colleague who stood next to them. At that particular moment, their surrounding trumped cybersecurity sharing knowledge. This highlights the importance of understanding the context of the behaviour. A 2020 research report by Tessian found that protecting information is more challenging when users are working remotely, attributing the absence of the IT team as one of the root cause (Tessian, 2020) – this is also in line with

Oltsik (2020). Kirlappos et al. (2015) argue that if the required cybersecurity behaviour impeded their job performance, employees will cut corners when it comes to adhering to cybersecurity policies. In most cases, they will exhibit positive cybersecurity behaviours.

2.2.4 *Proposition 2*

This study posits that remote working increases naïve mistakes and that not all embedded cybersecurity behaviours are carried to the remote workplace.

2.3 Which cybersecurity behaviours are carried to the remote work environment

Economic and social psychology disciplines have produced a significant body of literature, research, and understanding on human behaviour in organisations. Many hypotheses have been proposed, many occurrences have been investigated and reported on, and many theoretical underpinnings have been established as a result of these studies.

2.3.1 *Defining cybersecurity behaviour*

Psychology defines behaviour as human interaction of their environment (Popescu, 2014, p. 2). Cybersecurity behaviour falls under the human aspect of cybersecurity, a subsect cybersecurity that focuses on how humans interact with technology, policies and the organisation (von Solms & von Solms, 2018). This is a growing field because historically, cybersecurity focused on the technology – the tools and systems put in place to protects organisations against cybersecurity risks (ENISA, 2019, p. 6) – ignoring the integral part humans play in the implementation and success of cybersecurity technology (Furnell & Clarke, 2012; McCormac et al., 2017).

2.3.2 *What influences cybersecurity behaviour*

Much research has given attention to identifying sources of cybersecurity behaviour that impact the organisation to predict future actions. Professionals in cybersecurity predominately see employees who violate cybersecurity policies as Achilles' heels that constantly search for methods to make them compliant. Many therefore consider psychology and behavioural economics as potential avenues to help people to take cybersecurity seriously. Borrowing from these disciplines, efforts to drive certain employee behaviour tend to be nudges that utilise methods such as framing (Caputo et al., 2016) or command and control (Kirlappos et al., 2015).

The theory of planned behaviour is widely used to study the factors influencing cybersecurity behaviour. The theory argues that an employee establishes that the required behaviour is positive (attitude), and those around them support behaviour (social influence), which will motivate them to perform the behaviour. The theory added that employees also assess their capability to perform the behaviour (self-efficacy) and if they believe they can perform the behaviour, they will most likely do so (Ifinedo, 2014; Sohrabi Safa et al., 2016). Despite being a good tool, measuring behaviour is complex and the theory ignores the influence of organizational measures. Organisation factors create objectives that can lead to employees not complying with cybersecurity policies (Kirlappos et al., 2015). This study reviewed various publications and established that the decision of an employee to follow cybersecurity policies behaviours is impacted by his/her work objectives, perspectives, attitudes and norms.

that presented strong arguments for constructs such as attitudes or personality features that are assumed to influence whether people behave the way the organisation expects them to behave. These studies present strong arguments that there are relationships between these constructs and behaviour and that there are correlations between some characteristics between humans and desirable and undesirable behaviours. The next sections identify these factors.

- **Attitude** is the positive or negative mindset of the person to engage in an expected cybersecurity behaviour (Benbasat, 2010; Ifinedo, 2012).

Attitude is a predictor of behaviour as argued by Ajzen and Fishbein (1973) stating that a positive attitude toward cybersecurity policies will most likely influence intentions to behave positively. Various reports have repeatedly supported the impact of mindset on cybersecurity behaviour (Herath & Rao, 2009; Ifinedo, 2014).

- **Self-Efficacy** the confidence a person has in their capacity to complete a task or an action (Schwartz, 2012). In a security context, employees with mature levels of self-efficacy are often more adhere to the required cybersecurity behaviour because they believe in their capability to learn that stems from their effective learning mechanism (Herath & Rao, 2009). Benbasat (2010) argue that self-efficacy influences an employee's intention to comply with cybersecurity policies, which leads to the actual behaviour is positive.
- **Social influence** is the degree to which the action of a person is affected by what they believe others (e.g. family, friends and colleagues) are doing and the extent they want to follow that behaviour. Social influence has been shown to alter the cybersecurity behaviours of employees in a work setting. If most employees in the office environment behave securely, it will influence other employees to follow this behaviour because of the notion that this behaviour is expected (Bulgurcu et al., 2010) Consequently, the workplace environment of workers and people in this environment are essential factors of cybersecurity behaviours (Ifinedo, 2014).
- **Organisation factors** are initiatives put in place by the organisation to drive basic hygiene behaviour. Companies mainly rely on cybersecurity policies which enforced using awareness and training (D'Arcy et al., 2009). Researchers have found mixed results on the impact of cybersecurity policies on basic hygiene behaviour Lee et al., (2004) found that cybersecurity policy had little influence on basic hygiene behaviour. Researchers have argued that this is influenced by a lack of employee cybersecurity awareness therefore businesses have relied on awareness and training(D'Arcy & Devaraj, 2012).

2.3.3 *Hypothesis*

Based on the above discussions, the study hypothesises that organisation factors will have the strongest impact on cybersecurity behaviour. Therefore:

H1: There is a relationship between personal attitude and remote worker's intent to comply with cybersecurity policies.

H2: There is a relationship between social influences and remote worker's intent to comply with cybersecurity policies.

H3: There is a relationship between sense of control and remote worker's intent to comply with cybersecurity policies.

H4: There is a relationship between organisation factors and remote worker's intent to comply with cybersecurity policies.

2.4 Conclusion of Literature Review

This literature review introduced cybersecurity and the challenge that it presents to organisations. Previous research on the topic was discussed, gaps in literature were highlighted and the need for this study was argued.

2.4.1 *Proposition 1*

The first proposition posits that through cybersecurity policies and guidelines, organisations embed basic hygiene behaviours in the office environment.

2.4.2 *Proposition 2*

Remote working increases naïve mistakes there not all behaviours are carried to the remote workplace.

2.4.1 *Hypothesis 1*

Organisation factors, employee attitudes, social influence and sense of control influence complaint behaviour

2.5 ANALYTICAL FRAMEWORK

2.5.1 *Theoretical Framework*

a. *Compliant Behaviours in the office environment*

To understand the behaviours organisations enforce when employees work within their company premises, the study made use of work by Parsons et al., (2014). Using Jason's taxonomy of behaviour, Parsons et al., (2014) categorised expected compliant behaviours that companies put in place using cybersecurity policies as well as training and awareness initiatives. Parsons et al., (2014) argued that behaviours companies enforce usually fall within these categories: password management, e-mail use, internet use, social networking site use, incident reporting, working remotely and information handling. The tool is widely used to assess employee knowledge of cybersecurity policies and was used in this study to guide the thematic analysis to put codes into themes. The aim of this research is not to test the tool itself but to use it as a guide to categorise codes that emerge from interviews. The use of this model is also driven by literature arguing that cybersecurity behaviours are usually limited to one or two whereas this model encompasses a group of behaviours.

b. *Factors influencing behaviour*

Behaviour change models provide a good standing ground for understanding factors that drive cybersecurity behaviour. The Theory of Planned Behaviour – attitudes influence behaviour – and Protection Motivation Theory – the level of risk stemming from behaviour and avoiding these - are amongst the most widely used theories when it comes to understanding the human factor in cybersecurity (Ifinedo, 2012).

Ajzen & Fishbein (1973) presented sub-constructs to measure influences of behaviour: (i) attitudes towards behaviour; (ii) subjective norm, perceived effects that others may impose on behaviour; and (iii) perceived behaviour control, to the degree to which individuals think they can regulate social behaviour performance. Researchers argue that employee cybersecurity behaviour is also influenced by

organisation factors such as task objectives and training received by the organisation which then influences the aforementioned constructs (Kirlappos et al., 2015). Therefore, organisational factors play an integral role in the behaviours of employees. This was used in the development of the theoretical framework that will help uncover factors that influence cybersecurity behaviours in the remote workplace.

2.5.2 *Conceptual Framework*

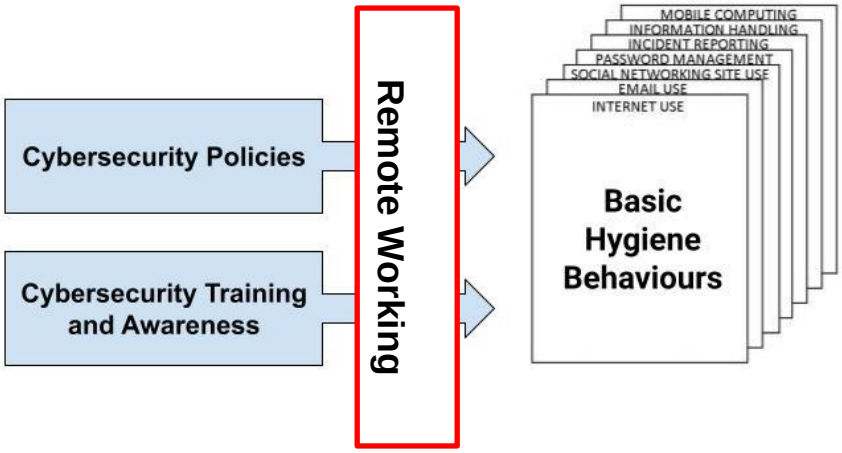


Figure 5 categorising behaviours enforced in the workplace. Adopted from Parsons et al., 2014 (2014)

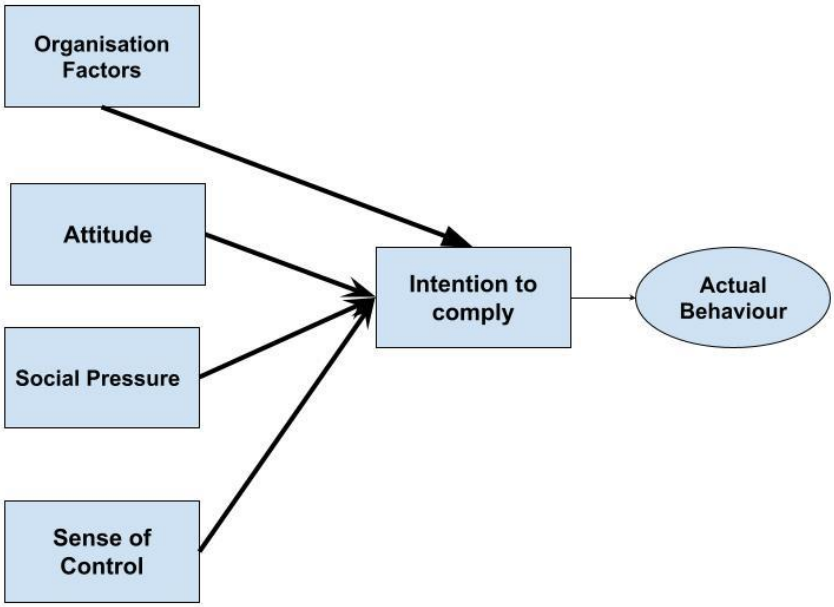


Figure 6 factors influencing cybersecurity behaviours. Adopted from (Ajzen & Fishbein, 1973)

CHAPTER 3. RESEARCH METHODOLOGY

This chapter discusses the approach taken to investigate the research problem stated in chapter 1. The research approach and design are discussed first, followed by the research sample, population and methods and data collection methods which are described in-depth, as well as the data analysis procedures. Following that is a description of the research's ethical considerations and limitations. Each section is supported by the rationale behind each decision.

3.1 Research approach

Research approach series of steps taken by the researcher in for the process of gathering, synthesizing, analyzing, interpreting, and reporting on the data collected (Tashakkori & Teddlie, 2003; Abbas Tashakkori & Teddlie eds, 2010; Abbas Tashakkori, Teddlie, Plano Clark, & Badiee, 2015). It forms the guiding principles that the researcher uses in their journey to answer the research questions and provides insight into the logic utilised by the researcher to make interpretations when the study is concluded.

This study adopted a mixed-methods design to answer the research questions, which allowed for a holistic view of the problem. Mixed-methods design is a research approach that seeks to answer the research question by collecting and analysing both quantitative and qualitative data. Research questions and design are two important characteristics of a mixed-method study. While research questions inform what we are seeking to understand about a phenomenon, they also inform the design chosen to conduct the study. To answer their research questions, researchers explored various methods to collect and analyse data (Morris & Burkett, 2011). The research methods are usually predetermined, and the methods are planned before undertaking the research. Since its inception, these research methods have developed into two distinct categories: quantitative and qualitative (Fetters, Curry, & Creswell, 2013).

A quantitative approach is best if the issue involves defining variables that affect an outcome, evaluating the utility of an action, or determining the best predictors of outcomes. It is also the perfect way to bring a hypothesis or explanation to the test (Guetterman, Fetters, & Creswell, 2015; Tashakkori & Teddlie, 2010). Quantitative research tends to lean towards reliability and validity to make the outcome of the study replicable by other researchers. It does, however, fall short of capture complex subjects as well as being flexible after the method is chosen(Leech & Onwuegbuzie, 2009; Tashakkori, Teddlie, Plano Clark, & Badiee, 2015). In this approach, the researcher's position is that of a neutral observer, and every attempt should be made to reduce the possibility of the researcher personally influencing or biasing findings (Lincoln, Lynham, Guba, & Others, 2011).

In contrast, a qualitative approach is necessary where a topic or phenomenon needs to be investigated and clarified because there has been no study on it or the research involves an understudied sample (Creswell, 2007; Kroll & Neri, 2009). This approach is also important when the group or sample being studied have no existing theories to suit them (Creswell, 2007). In this approach, the researcher's position is to reach the thoughts, feelings and experiences of participants (Lincoln et al., 2011). Qualitative research dives deeper by providing rich insights that may have been missed by quantitative research (Creswell, 2013). It does, however, have shortcomings when it comes to objectivity, transparency, and generalisation (Bryman, 2006).

In attempting to uncover the role of remote working on cybersecurity behaviour, the researcher identified that research focusing on the human aspect of cybersecurity is predominantly conducted in the office environment (ENISA, 2019). Researchers who have conducted have studies on cybersecurity behaviour have mainly focused on the home user (B. Y. Ng & Rahim, 2005; Talib, Clarke, & Furnell, 2010) and focusing on personal computer usage. Very little research is conducted on understanding whether behaviours change outside the company premises (Furnell & Shah, 2020). The research question, therefore, guided the need to apply a mixed-methods research approach. To understand the role of remote working on cybersecurity behaviours, the study identified three

underpinning objectives – understanding how employees behave in the workplace (qualitative), whether this changes in the remote working environment (qualitative) and understanding factors that influence their behaviours (quantitative). Bryman (2006) highlighted the benefits of using mixed methods due to its ability to draw on strengths from quantitative and qualitative methodologies while eliminating their pitfalls.

Where a quantitative or qualitative approach is insufficient for a clearer understanding of a research problem, a mixed-method design is helpful (Hanson, Plano Clark, Petska, Creswell, & Creswell, 2005). The strengths both of quantitative or qualitative research and its associated data provides a better analysis. Creswell (2007) argues some researchers have a goal to generate a clear understanding of a phenomenon or definition for individuals and generalize their findings to larger a population. Having assessed the research problem and the underlying questions, it was established that the study would benefit from a mixed method. The question “What is the role of remote working on cybersecurity behaviour” could not be comprehensively answered without relying on both methodologies.

3.2 Research design

The research adopted a concurrent mixed-method study because sub-questions were established from the start (Tashakkori & Creswell, 2007). Creswell and Plano Clark (2018) argue for three main types of mixed methods research questions namely explanatory, exploratory, and convergent. Mixed-method studies are based on explanatory or exploratory research questions that make use of sequential design i.e., either quantitative or qualitative data will first be collected and then the other data will be collected. Likewise, a convergent research question generally involves a simultaneous design in which quantitative and qualitative data are gathered at the same time (Creswell, 2013). When the research question is convergent mixed methods the quantitative and qualitative data can be collected at about the same time and are then used together to triangulate the findings and answer the research question one of the challenges. Figure 8 below shows the convergent mixed-method process. It usually involves

the gathering and analysis of quantitative and qualitative data simultaneous but independent in line with the research questions to enable the researcher to better grasp the topic of inquiry (Tashakkori & Creswell, 2007). This subsequently enables the researcher to amalgamate results from two datasets. The overarching question, *"Do behaviours enforced in the office environment transfer to the remote work environment"* was spilt into sub-questions that had qualitative and quantitative strands (Creswell, 2007). (Koskey & Stewart, 2014). The goal of employing this approach is to integrate the various strengths and limitations of quantitative methods (generalisation, correlations and larger sample size) with those of qualitative methods (in-depth understanding, the details and smaller sample size) (Tashakkori et al., 2015). Convergent design is used to either make comparisons between quantitative statistical results and in-depth qualitative results as well as validate quantitative results or expand qualitative results. The goal of this study was the latter, mainly given the fact that research shows disparate views on cybersecurity behaviour between the organisation – represented by cybersecurity professionals – and end-users – non-IT staff (Kirlappos et al., 2014; Pfleeger et al., 2014). The data were collected and analysed separately and integrated during the discussion phase. This approach was intended to lead to reliable and well-founded findings of cybersecurity behaviours in the remote environment (Fetters et al., 2013). Despite using a mixed-method, more weight was given to the qualitative strand because two of the questions – focusing on behaviours in the work environment vs behaviours in the remote working environment – were predominantly qualitative.

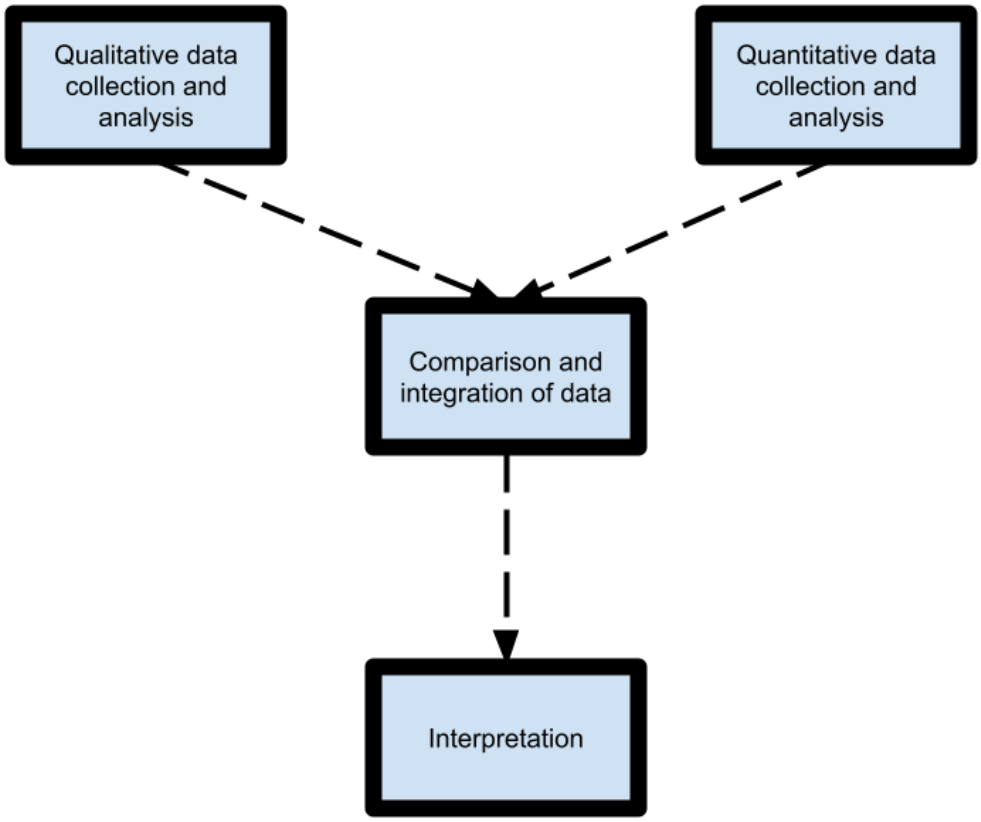


Figure 7: Convergent mixed-method study (Fetters et al., 2013)

3.3 Data collection methods

The data collection method is usually driven by the research question, objectives and gaps identified in the literature (Creswell, 2009; Creswell & Poth, 2016). It is well documented that there is more need for qualitative or mixed methods research in research focused on cybersecurity behaviour (Kirlappos et al., 2015). In addition to observations and document analysis, interviews are regarded as an invaluable source of information when conducting qualitative research (Venkatesh et al., 2016). Interviews can be unstructured, semi-structured or structured. Semi-structured interviews provide in-depth information about the research problem by enabling the researcher to prompt for more insights from the interview where necessary. This helps address individual opinions and descriptions of individuals themselves and gain from finding questions or concerns which the researchers did not anticipate - leading to more flexibility in a

structured approach (Creswell & Poth, 2016). Cybersecurity is a sensitive subject to most, especially when non-compliance behaviour is discussed (Adams & Sasse, 1999; Kirlappos et al., 2014). It was imperative to use semi-structured interviews to enable the researcher to adjust to the interviewee's level of comfortability.

Survey questionnaires were utilised for the quantitative element of the research. Survey questions enable a collection of quantitative data at a single point in time to provide a snapshot of a phenomenon (Bryman, 2006). Surveys help answer:

- Descriptive question – what factors influence behaviours?
- Relationship questions – is there a correlation between cybersecurity behaviours and leadership?
- Questions regarding the predictability of variables across time – Does BYOD influence behaviours over time?

One of the research objectives was to use uncover factors that influence cybersecurity behaviours in the remote workplace. For this objective, survey questions underpinned by a modified theory of planned behaviour was used to uncover the most influential factor (Godlove, 2012). A was chosen because it is quick to turn around and inexpensive as opposed to other methods (Creswell, 2013). Using the questionnaire data, patterns from the variables were investigated and establish key patterns and correlations (Bryman, 2006). Data was collected was cross-sectional by taking a snapshot at one point in time (Rindfleisch, Malter, Ganesan, & Moorman, 2008).

3.4 Population and sample

This section discussed the rationale behind the chosen population and the sampling techniques applied.

3.4.1 *Population*

The role of remote working on cybersecurity behaviour was limited to the financial services industry to increase feasibility. The financial services sector was the

focal point of interest given how regulated they are and attractive they are to malicious attackers (Terekhova, 2018).

Respondents were geographically based in South Africa and were employed in the South African Financial services. Cybersecurity professionals (qualitative) were required to be an employee within the financial services sector for more than two years to ensure that they had enough experience about the behaviours within the office environment and the remote environment. will have to be working from locations outside the company premises. Should they work from the office at the time of the interview, they must have been working remotely for at least 3 months as per national lockdown regulations.

3.4.2 *Sample and sampling method*

Sampling is a crucial step in the analysis process that helps to evaluate the inference accuracy that researchers produce and affects the extent to which results can be generalized to a larger population (Onwuegbuzie & Collins, 2007; Teddlie & Yu, 2007; Venkatesh et al., 2016). Researchers who employ a mixed-method investigation must make assessments about the sampling elements of both the qualitative and quantitative methods (Collins, Onwuegbuzie, & Jiao, 2007). Sampling methods can be categorised and grouped by the type of mixed-method research they can be grouped into – concurrent or sequential (Venkatesh et al., 2016). Venkatesh established four types of mixed-methods sampling that studies, namely basic, sequential, concurrent, and multiple sampling designs. Basic sampling methods consist of probability sampling, stratified purposive sampling, and purposive sampling. Probability sampling is a common component of basic mixed-methods sampling techniques. Using this method, the sampling units that represent the population are chosen at random by the researcher (Collins, 2015).

Stratified purposive sampling, also known as a sample within a sample, is a strategy whereby the researcher segments the population of interest into strata and then use a purposive sampling method to pick a limited number of cases to research intensively in each stratum. Quantitative experiments are most likely to use probabilistic sampling structures, whereas qualitative studies use purposive

sampling designs. Argues that both probabilistic and purposive sampling strategies can be utilised in both quantitative and qualitative research (Venkatesh et al., 2016). Sequential sampling strategies involves utilising techniques and findings from the first strand to guide the approach used of the second strand. For example, utilising qualitative data to form constructs that can be measured utilising quantitative methods. Concurrent sampling techniques help researchers to triangulate the results from the different quantitative and qualitative components of their studies and to confirm, cross-validate or corroborate their findings in a single sample. Multiple sampling strategies generally involve integrating one sampling method with another. For example, making use of concurrent mixed methods on playing with stratified purposive sampling.

This research made use of concurrent sampling methodology by using parallel sampling techniques. Venkatesh et al., (2016) argue that when the samples for the quantitative and qualitative elements of analysis are separate but taken from the same underlying population, this is known as parallel sampling. The chosen population was cybersecurity employees in the South African financial services sector, the quantitative sample derived from financial services employees (end-users and non-cyber security staff) who are required to adhere to cybersecurity policies and cybersecurity professionals within the financial services sector who are responsible for implementing and monitoring the employee's cybersecurity behaviour. The purpose of this decision was driven by the notion – based on the researchers own work experience – that cybersecurity noncompliance behaviour is considered taboo which may influence their ability to speak openly about the subject matter. Therefore, hearing changes in behaviour from those responsible for monitoring the cybersecurity behaviours of employees was going to give the data more meaning.

i. *Qualitative element*

During the process of determining the study sample for the role of remote working on cybersecurity behaviour, necessary biases were considered. Each organisation, no matter the size, work toward a standardised approach to ensure uniform cybersecurity behaviour. Therefore, have too many participants from a

single organisation could have resulted in biases from organisation culture and limit the richness of data (Fetters et al., 2013). This would have introduced limitations in making the study represent the overall population. The researcher avoided this by putting a cap on the number of participants per organisation to a maximum of 2. The researcher also anticipated that seniority level and as well as roles and remit could have influenced data quality because junior cybersecurity employees within the IT department may not have had the necessary experience to draw from.

Purposeful sampling used to curb the aforementioned biases and increase data richness (Fetters et al., 2013; Onwuegbuzie & Collins, 2007). An additional criterion was added to ensure that all participants should have been an employee at their company for more than two years – this enabled them to have enough observations about employee behaviours in the workplace before the national lockdown in March 2020 – and the changes in behaviour since if any. This was made possible by investing in a LinkedIn Sales Navigator licence – more on this in the data collection procedure.

The total population of this study was financial services companies with a head office in one of the nine provinces in South Africa. For this study, financial services refer to companies within the following categories:

- Banks
- Insurance companies
- Investment services
- Asset Management companies
- Accounting and consulting
- Speciality Finance

For the qualitative method, the target group was those who administer the policies. For both groups, we will use purposeful sampling which focuses on a set criterion driven by the purpose of the research.

The target sample was:

- 8 members of IT teams, responsible for putting policies that drive behaviour in place. They must work in cybersecurity and responsible for ensuring policy compliance (LinkedIn Sales Navigator enabled this criterion to be executable).

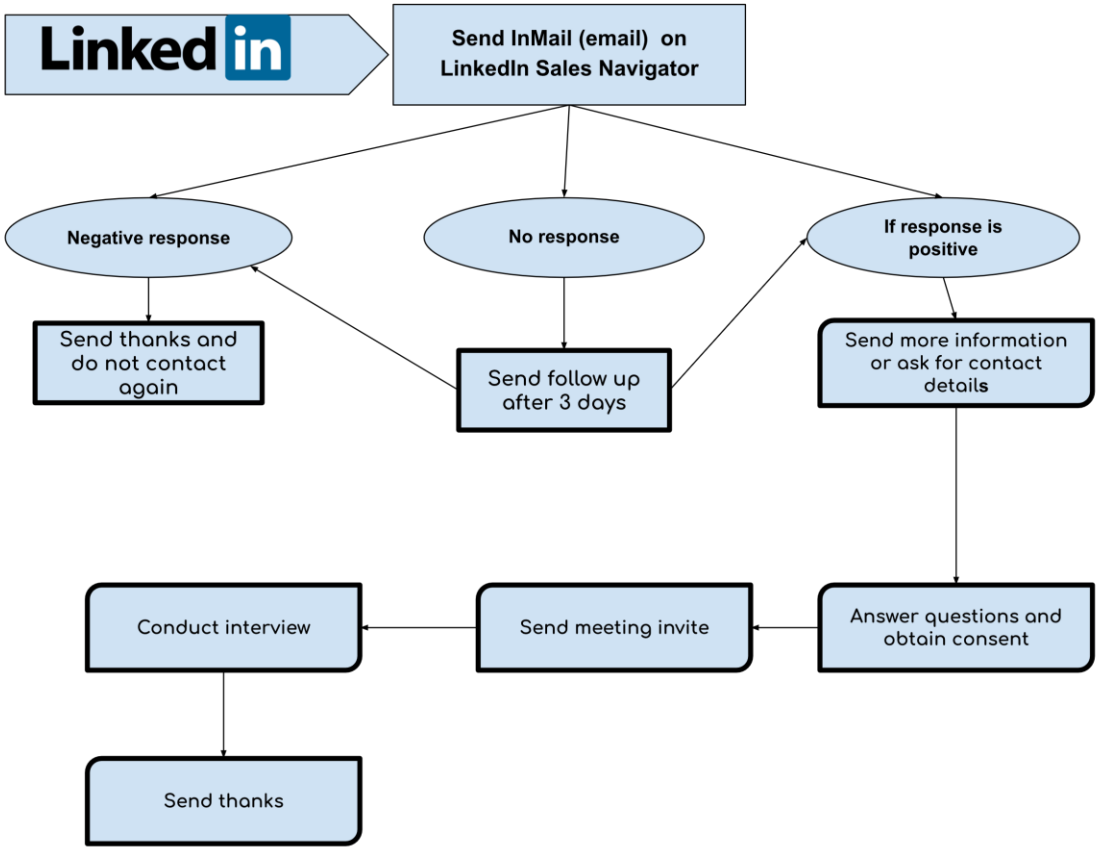


Figure 8: data collection process for quantitative data

The desired total number of interviews was 8. When it comes to qualitative research, there is an argument that the sample size depends on the research question. It is argued that in qualitative research the sample size should be driven by data saturation (the point where themes are repeated and there is not new information) which the sample size of 10 feels adequate (Baker, 2018).

ii. *Quantitative element*

For the quantitative method, random sampling was deployed. Quantitative data gathered in this research was obtained from a group of current financial services employees via LinkedIn. LinkedIn was used as the main platform to distribute the

survey. The researcher was given access to Bankers & Finance Professionals of South Africa, a professional group consisting of financial services professionals. LinkedIn users are required to go through a screening process before being granted access to this group.

The group's membership consists of over 5000 employees within the financial services sector. Each day, The researcher was allowed to post weekly reminding group members to take part in the survey. For accurate evaluation of psychometric, including test-retest reliability and internal consistency, Kline (2013) suggested a minimum of 100 participants from a representative sample, which is considered a prerequisite for adequate construct validity.

3.5 The research instrument

Mixed method research instruments and strategies were driven by the nature of research questions. Venkatesh et al., (2016) argue that this can be driven by their open-ended questions (asking employees about their attitudes towards cybersecurity), open-ended questions (asking them to talk openly about cybersecurity behaviour) and emphasis on numeric data analysis. The researcher needs to be aware of the shortcomings and strengths of each method and leverage this to enhance the quality of the research.

i. *Qualitative Instrument*

The semi-structured interviews (Appendix B) were designed to answer two of the qualitative questions. The questions focused on understanding the behaviours that companies have put in place through policies and uncover whether these behaviours carried to the remote working environment.

Questions focused on the following elements discussed in the literature review:

- Uncovering behaviours classified as malicious or good behaviour.
- How these behaviours are enforced – training
- How these are put in place

- How employees behave in the workplace
- How this changes in the remote workplace
- What caused the change or non-change in behaviour.

An interview protocol was used to collect data and guide the interview process. The interview protocol was used to generalise by making sure that all questions are posed to all participants. Details are discussed further in the data collection process (Lietz, 2010). The choice of semi-structured interviews was due to their nature of keeping the respondents view while allowing the researcher to make or adjust their questions during the interview. This allows for rich insights to increase the validity of the research (Creswell, 2009).

ii. *Quantitative Instrument*

To uncover the factors influencing changes in behaviour, the research made use of a modified Theory of Planned Behaviour research instrument focused on teleworking employees. A customised 21-item Remote Working Survey (Appendix D) was developed created to measures four independent variables (social influence, personal attitudes, social influence, perceived sense of control and organisational factors) highlighted during the literature review. The questions customised 21-item remote working survey measures key components of the theory of planned behaviour in a Likert scale ranging from 1 being strongly disagree to 5 strongly agree. This instrument was developed as an adaptation of the Teleworker Security Survey used by Godlove (2012).

3.6 Procedure for data collection

i. *Qualitative data*

Qualitative participants (cybersecurity professionals) were selected using LinkedIn sales navigator, a paid-for premium version of LinkedIn that enables the user to reach out to individuals not part of their network. The research conducted

an InMail campaign asking for permission to be interviewed. A total of 60 of these InMails were sent to two participants that met the criteria mentioned in the sampling method. The researcher also made attempts to contact organisations directly, however, due to the covid pandemic causing most organisations to shut down headquarters, contacting human resources professionals proved to be a challenge. A total of 16 participants responded showing interest with the majority requesting the questions ahead of agreeing to participate.

The researcher requested their contact details and follow these up by sending the questions, a bookable calendar link, and ethics clearance confirmation. Fourteen participants agreed to proceed with the interviews and ten interviews took place. Two interviews were disregarded due to the participants not being able to obtain clearance from their respective organisations, despite being guaranteed anonymity. The researcher did not include a screening call and preceded with conducting interviews. the thought process behind this decision was to create a pool of insight that enabled the researcher to pick from. A total of nine interviews took place, with the remaining four participants facing delays or rescheduling to a date that would not meet this submission deadline. One interview had to be omitted due to a last-minute request from the participant to exclude their insights. The researcher made use of Microsoft Teams as a medium to conduct the interviews. Before commencing the interview, participants were given a brief background of the purpose of the research, given the opportunity to ask any further questions and given a brief overview of how their data will be protected and used. The next step was to get their consent to proceed with the interview followed by the commencement of recording the interview.

The first interview took place on December 20, 2020, via Microsoft Teams. There was a lengthy break between the third and fourth interview due to other participants dropping off because of work commitments and the researcher falling ill after testing positive for Covid-19. Microsoft Teams keeps a transcribed copy of the call if the user selected OneDrive as the destination folder. The participants logged into the call using their computers, with two participants dialling in from their mobile phones. The participants who dialled in using their mobile phones faced connectivity issues, which hampered the fluidity of the conversation –

virtual meetings needed to be restarted whenever this occurred. Transcriptions were not 100 per cent accurate due to various factors such as employee microphone picking up background noise, connectivity issues requiring the meeting to be ended and restarted and load shedding that occurred on the researcher side during one interview. To remedy this, all call transcription generated by Microsoft Teams were screened before the data analysis phase to remedy any discrepancies. (interview process steps included in Appendix B)

ii. *Quantitative data*

The remote working cybersecurity survey questionnaire was built using Qualtrics and distributed via sharable links. Quantitative data gathered in this research was obtained from a group of current financial services employees. LinkedIn was used as the main platform to distribute the survey. The researcher was given access to Bankers & Finance Professionals of South Africa, a professional group consisting of financial services professionals. Before being given access to the group, LinkedIn users are required to go through a screening process before being granted access to this group. The group description is described as follows *"A networking group for banking and financial services professionals of South Africa: if you work in a bank or for a wealth manager or in any other financial setting, join to discuss changes in the market, job opportunities and link with like-minded individuals in your local area."*

The group's membership consists of over 5000 employees within the financial services sector. Each day, The researcher was allowed to post weekly reminding group members to take part in the survey. A total of 76 respondents took part in the survey and 63 completed it. This was a lower than planned number.

3.7 Data analysis and interpretation

In the mixed-methods study, three techniques for data analysis may be used, depending on the order of data analysis. These methods occur when both

qualitative and quantitative data are analysed at the same time (simultaneous mixed analysis), qualitative data is analysed first followed by quantitative data (sequential qualitative-quantitative data analysis), and when quantitative data is analysed first followed by qualitative data (sequential quantitative-qualitative data analysis). The study followed concurrent mixed-method principles therefore qualitative and quantitative data were collected and analysed separately (Bryman, 2006; Creswell, 2007; Creswell & Creswell, 2018; Tashakkori & Teddlie, 2003).

This study made use of a hybrid inductive and deductive approach to analyse data (see figure below). Fereday and Muir-Cochrane (2006) used this method to aid their study's theme development. The rationale for using this approach was to help answer the first sub-question, *what behaviours are enforced in the office environment* by the group the codes into categories and eventually into themes. Previous cybersecurity studies have fallen victim to focusing on a single behaviour that has been found to not be a true account of the phenomenon (Kirlappos et al., 2014). Therefore, the deductive element was purely used to guide the group on the types of cybersecurity behaviours enforced in the office environment. The HAIS questionnaire is widely used to categorise groups of behaviours when a study isn't focused on a single behaviour – e.g locking screens (Pattinson et al., 2015).

Inductive analyses, which are primarily descriptive and exploratory, were used in the qualitative component of this study. Despite the existence of confirmatory approaches to qualitative data analysis, social/behavioural research tends to favour exploratory and industrial analysis. An exploratory analysis involves the researcher carefully reading the data to identify key phrases, patterns, themes or ideologies within that the text before conducting further analysis (Guest, MacQueen, & Namey, 2011). This benefited the second sub-question, which behaviours are transferred to the remote workplace, where behaviours mentioned in sub-question one was compared to behaviours in sub-question two. Themes identified inductively emerge directly from the data, whereas themes identified deductively relate to a predetermined model or theory (Nowell, Norris, White, & Moules, 2017). Using Quirkos (see Appendix C), each transcript was

formatted uploaded on the software. Each question was formatted using a heading style and responses from participants were left as body text – time staps with emoted from the transcript but the word interview stayed to indicate that the interview is speaking at that given point.

Thematic analysis was used to identify key themes in our study. As one of the most flexible methods in qualitative research, it allows the researcher to gather insights that are rich and detailed (Braun & Clarke, 2006). Guided by the study, the following steps were followed (see figure 9):

1. Being familiar with the data
2. Generating initial codes
3. Identifying themes
4. Reviewing the identified themes
5. Defining and naming the themes
6. Writing the report

Thematic analysis is a widely used approach in psychology that has gained significant acknowledgement as a qualitative analytic technique in its own right (Guest et al., 2011). The themes identified during the analysis phase mainly focused on the inductive analysis given that the interview questions did not heavily rely on existing theories of cybersecurity behaviour in the remote workplace (Baer et al., 2008).

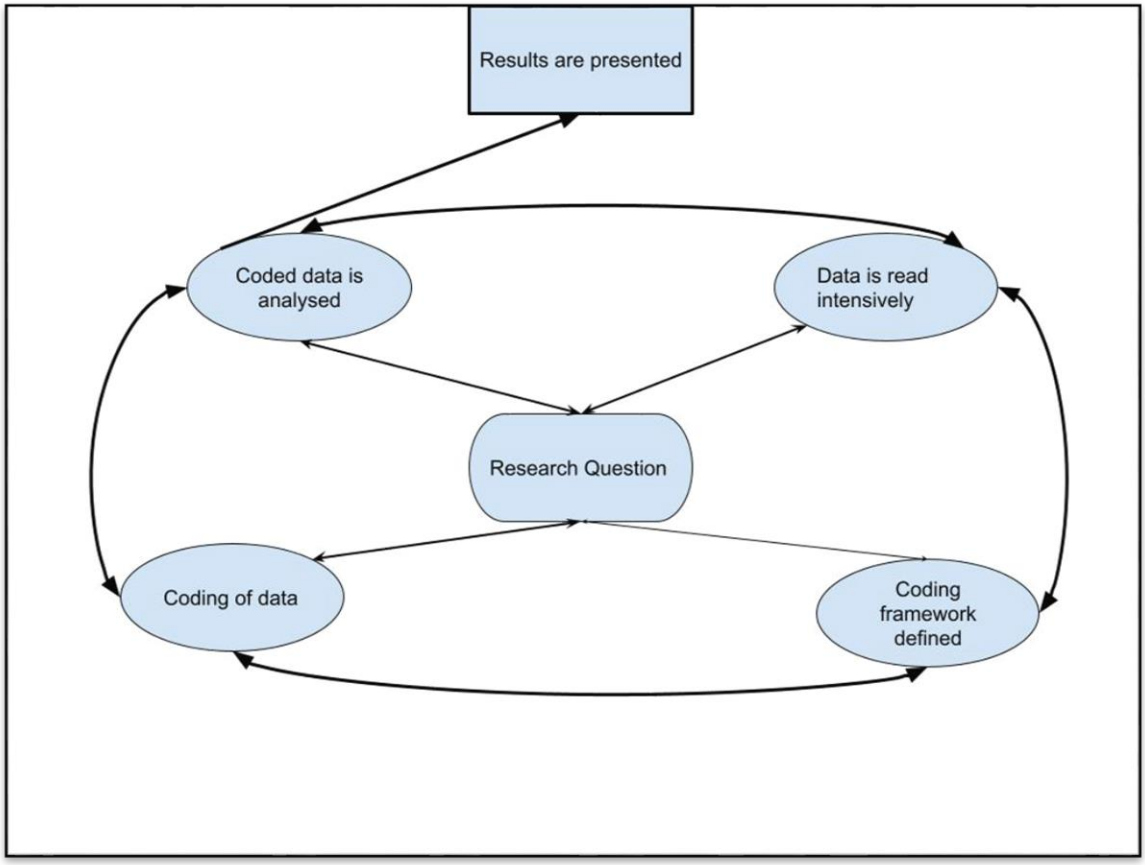


Figure 9 coding process informed by Braun & Clarke (2006)

i. *Quantitative Data*

To identify any relationships and grouped differences in survey items and composite scale scores, descriptive and inferential statistical techniques were used to analyse the survey data (Creswell & Creswell, 2018). The findings of the personal attitude, social influence, feeling of control, and organisational measure scales were analysed using regression analysis to see how well they explained intent to follow an organization's cybersecurity rules.

3.7.2 Definitions of variables

The theory of planned behaviour was used to operationalise the independent and dependent variables. The dependent variable was intention to comply with cybersecurity policies when working remotely. A 5-point Likert scale focusing on intention was used to operationalise the variable. The independent variables

consisted of a 6 item Personal Attitude scale, 5 item Social Influence scale, 5 item Sense of Control and 4 item Organisational Factors and were operationalised used a 5-point Likert scale.

The participant's agreement or disagreement with comments about remote working was assessed using Personal Attitude. This section concentrated on remarks on being aware of the effects of cybersecurity risks and the need for safe cybersecurity behaviour.

The social pressure scale measured a participant’s agreement and disagreement with statements relating to remote working to the extent to which family members or friends and media such as consuming the news influenced their cybersecurity behaviour.

The sense of control scale measured a participant’s agreement or disagreement with statements relating to remote working to the extent to which they believed that their behaviours increased or decreased cybersecurity risk, cybersecurity was an IT only problem and whether they believed that complying with cybersecurity behaviours is easy.

The Organisational Factors Scale measured a participant’s agreement or disagreement with statements relating to remote working to the extent to which they believed that their organisation’s support towards ensuring compliant behaviours is well communicated and easy to follow.

3.7.3 *Data analysis procedure*

Both descriptive and inferential procedures were implemented to establish relationships as well as group differences in scores on the survey items and its composite scores. To determine how well the scores on the Personal Attitude, Social Control, Sense of Control and Organisational Factors scales explained the intent to continue complying with cybersecurity policies, the research employed regression analysis.

3.7.4 *Methods of data analysis*

Data collected from Qualtrics were exported into excel and assessed to ensure validity and account for incomplete data points. The next step was to establish if any significant relationships existed between the dependent (intent to continue complying with cybersecurity policies in the remote workplace) and independent variables. This analysis was conducted using Microsoft Excel's data analysis tools. An additional step was to conduct a regression analysis to examine how well the four independent variables explained the dependent variable.

3.8 Limitations of the study

- Despite its growing popularity, mixed methods research thematic analysis falls short because it lacks clear guidelines. This lack of clear guidelines means that anything goes which may limit the research findings (Braun & Clarke, 2006).
- This study would have benefited from sequential mixed method research by first collecting data from interviews with cybersecurity professionals and using that to formulate a quantitative instrument. Due to time and resource constraints, a concurrent mixed method was used instead. as a result, the quantitative element of the research measured policy compliance with the assumption that it will encompass the behaviours identified in the first proposition.
- The survey link for the quantitative data was available to anyone with access to which resulted in respondent's self-selection – by showing interest in the topic and clicking on the link. Provision was made for this by asking respondents the industry in which they worked in which resulted in 22% of the respondent data not being used due to them not being in the financial services industry.
- Despite the smaller than planned quantitative being smaller than the target sample, argument can be made for this being a good indicator of the population because there was no incentive in taking part in the survey other than showing genuine interest in the topic.

3.9 Validity and reliability/transferability and dependability

3.9.1 *Transferability*

The research meets transferability because it employs a detailed description of the respondents and research process which will enable it to be used in other scenarios (Korstjens & Moser, 2018). LinkedIn Sales Navigator was used to purposefully recruit participants for the qualitative element of research who are subject matter experts in the South African financial services sector.

3.9.2 *Credibility*

Persistent observation and member checks were used to guide the credibility of the research. Persistent observation will focus on factors pertinent to the problem (Braun & Clarke, 2006). Each participant received a detailed summary of the study during the debriefing phase to obtain consent (for those who requested emails, a summary email tailored to the participant was sent). The qualitative interview questions emerged from key themes identified during the literature review to guide the relevance of the questions to the remote working cybersecurity behaviour (Hanson et al., 2005). This guided the researcher's conclusions that common themes occurred during the sixth interview and saturation on the seventh interview. The design of the data collection and analysis phase ensured that triangulation was achieved (gathering qualitative and quantitative data, thus removing researcher subjectivity (Pardede, 2019).

3.9.3 *Reliability and dependability*

Due to the use of thematic design for qualitative analysis, which tends to lack clear guidelines, the research has adopted the guidelines from Braun & Clarke (2006) to increase dependability. It must also be noted that mixed methods increase validity by collecting qualitative and quantitative (Creswell & Creswell, 2018; Merriam & Tisdell, 2015). This process introduces a systematic approach to coming to answering the question. The strength of qualitative was anchored on validity. This was based on uncovering whether the data collected is accurate

from the perspective of the readers of the research, the researcher, and participants.

To increase the reliability of the quantitative survey instrument, a pilot test on the remote working cybersecurity survey was undertaken with a sample of six IT workers having cybersecurity as part of their mandate. (Creswell & Creswell, 2018; Onwuegbuzie & Collins, 2007). The IT professionals were required to participate in the survey and provide feedback on the structure, grammar, and length. The pilot testing aimed to establish areas that respondents might encounter challenges in completing the survey. Based on feedback from IT professionals, the final version of the survey went through adjustments to increase reliability and validity.

3.10 Demographic profile of respondents

Respondents were geographically based in South Africa and were employed in the South African Financial services. Cybersecurity professionals (qualitative) were required to be an employee within the financial services sector for more than two years to ensure that they had enough experience about the behaviours within the office environment and the remote environment. They needed to be working from locations outside the company premises at the time of the interview. Should they work from the office at the time of the interview, they must have been working remotely for at least 3 months as per national lockdown regulations.

The quantitative element of the research focused on remote working employees, also described as end-users. Demographic variables such as sex, age, ethnicity, location as well as other elements were not captured because they did not form part of the research objectives. The participants were required to be remote working employees in the financial services sector and must have been working remotely for at least 3 months as per national lockdown regulations.

3.11 Ethical considerations

Borrowing from Jung (2018), the following ethical guidelines will be formulated:

- The first step was to ensure that no physical or psychological harm was suffered by the participants. This was achieved through clear communication to the participants will be taken to ensure that this is achieved.
- The second was to ensure that the objectives of the research are clearly defined to the participants to drive informed consent.
- The third was ensuring that participant identities were not disclosed to ensure that there is no invasion of privacy.
- The last was ensuring that no deceptive methods are used to drive a predetermined end goal by the researcher.

Anonymity was crucial for the participant given the sensitivity of discussing cybersecurity. With this in mind, the researcher assigned each participant a number based on the order in which they took part in the research. Their privacy was given priority while ensuring the objectives of the research was achieved.

Before the data collection phase, the authorising committee granted the researcher ethics clearance. Microsoft OneDrive cloud platform was the primary storage location for all recordings to avoid data loss as a result of stolen computers, viruses, and hardware malfunction. The file naming convention was structured in an encrypted manner that was only relevant to the researcher. The OneDrive password was changed weekly and stored on Keeper (password management tool). The OneDrive account required a two-factor authentication to using Microsoft Authenticator on an IOS device that is iCloud protected. These steps were taken to enhance research credibility. Quantitative data was treated with care given the researcher's work remit being heavily reliant on following European Data Protection laws such as GDPR. This led to further research into the POPI act given that participants were based in South Africa. The acronym POPI stands for the Protection of Personal Information Act No. 4 of 2013. Parts of the law was passed on April 11, 2014, after being enacted on November 19, 2013. The rest of the legislation remained on the books but was no longer in effect

in 2019. It is expected to go into effect in 2019, depending on when the Regulator is fully operational (van Rensburg, 2020).

Table 1. Consistency table: research questions, propositions, data collection and data analysis

RQ #	State Research Question or Objective	Prop/ hyp #	Proposition or Hypothesis	Research questions	Data collection detail	Data analysis method
1	To understand the behaviours enforced in the office environment.	Prop. 1	Cybersecurity policies focus on driving basic hygiene behaviours	What cybersecurity behaviours do companies embed on employees through awareness and training when working within their premises	Interview guide questions 1,2,3,4,5	Thematic analysis
2	To understand whether the behaviour identified in research question 1 carry on to the remote workplace	Prop 2.	Working remotely will increase naïve mistakes	Which of these cybersecurity behaviours are transferred to the	Interview guide questions 6	Thematic analysis

				remote work environment?		
3	To uncover which factors influence employee cybersecurity behaviours when working remotely		Organisation factors, employee attitudes, social influence and sense of control influence complaint behaviour	What factors influence employee cybersecurity behaviours	Questionnaire: Likert statement	Description and Regression analysis

Table 1: Consistency Matrix

CHAPTER 4. PRESENTATION OF FINDINGS AND RESULTS

Introduction

Chapter 3 provided served as the research blueprint by expanding on the research design and methodology. The purpose of the research was to explore whether behaviours embedded within company office environments are carried over to the remote working environment. To answer this research question, it was imperative to understand the cybersecurity behaviours that organisations enforce within the office environment, uncover which of these cybersecurity behaviours are carried to the remote workplace and which factors influence these cybersecurity behaviours.

As a result, three research questions were presented in chapter 1. From the three research questions, propositions and hypothesis were presented which led to the research design being a mixed-method study – containing a quantitative and qualitative section therein. This chapter focuses on and explores the results of the analysis within the research framework. The qualitative element focuses on the findings derived from the results of a thematic analysis of the transcriptions obtained during the interview process with cybersecurity professionals. The quantitative element focuses on the results obtained from the survey questionnaire. Participant references were grouped into codes and the themes emerged from the codes.

The coding strategy is represented in Figure 10 below.

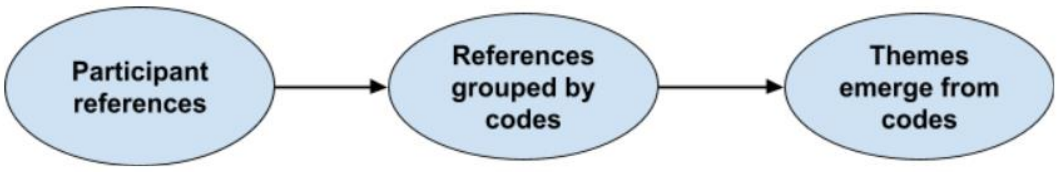


Figure 10 coding strategy

Table 2: How results fit into the Consistency Matrix

Research Question or Objective	Proposition or Hypothesis	Research questions	Data collection detail	Data analysis method & Emergent themes/Results
To understand the behaviours enforced in the office environment.	Cybersecurity policies focus on driving basic hygiene behaviours	What cybersecurity behaviours do companies embed on employees through awareness and training when working within their premises	Interview guide questions 1,2,3,4,5	• **Password Management** ○ Using strong passwords ○ Regularly change passwords ○ Never share passwords • **Information Handling** ○ Do not insert removable devices (such as USB's and DVD's) ○ Lock computer screen when unattended ○ Do not forwarding work-related information to personal email • **Email Use** ○ Never open email attachments and clicking on links from unknown sources • **Mobile Computing** ○ Always Use VPN ○ Never connect to public Wi-Fi for work

				○ Never share laptop with friends or family • **Social Network Sites** Use ○ Do not browse social media sites during work hours • **Incident Reporting** ○ Report incidents as soon as it occurs • **Internet Use** ○ Avoid dubious websites ○ Do not browse streaming websites
To understand whether the behaviour identified in research question 1 carry on to the remote workplace	Working remotely will increase naïve mistakes	Which of these cybersecurity behaviours are transferred to the remote work environment?	Interview guide questions 6	Basic hygiene behaviours that hinder productivity were bypassed
To uncover which factors influence employee cybersecurity behaviours when working remotely	Organisation factors, employee attitudes, social influence and sense of control influence complaint behaviour	What factors influence employee cybersecurity behaviours	Questionnaire: Likert statement	Results showed that personal attitude and sense of control had the strongest influence on employee behaviour than social influence and organisational factors

Table 2: consistency Matrix in relation to results

4.1 Results pertaining to Proposition 1

The purpose of this question was to uncover which behaviours are expected from employees in the workplace. The human aspect of the Information Security questionnaire (HAIS-Q) was used as a guide to categorise the behaviours into themes. Participants were asked to talk about good and bad cybersecurity behaviours within the workplace – in line with their respective cybersecurity policies. Their responses were captured as references and mapped with the questions on the human aspect of the Information Security questionnaire (HAIS-Q). HAIS-Q consist of seven focal areas that include Internet Use (IU), Mobile Devices (MD), Password Management (PM), Email Use (EU), Social Media Use (SMU), Information Handling (IH), and Incident Reporting (IR). The focal areas were further analysed into sub-themes to describe the behaviours in each category – see summary in figure 11.

Codes with common descriptions were merged renamed to formulate a broader definition. Given that the study's aim was not to verify, expand, or disprove the theory, the model merely served as a reference to the data analysis (Clarke and Braun 2014).

Table 3: Examples of codes derived from participant B about behaviours enforced in the office environment.

Codes	Example reference
Password Management	You know that our passwords length requires 8 characters, and they have to be alphanumeric?
Information Usage	So you know that if the CEO plugs in a USB after I've said that no USB is plugged, then you can take the same measures and take him to HR and say this person failed to comply.

Email Use	We would just send an email that has a phishing link and say you've won R2000, please go and click on this and then you would get your end as soon as the person clicks on that link
Incidence report	So I believe that you need to encourage people to come forth before you tell them what the ramifications are.

To reduce bias and influencing the themes, participants were asked questions about describe behaviours that are seen as positive behaviours and those that can be punishable. They were also asked about their training initiatives and the subjects covered in the training initiatives – this gave insights into most of the email behaviours. Lastly, participants were asked to discuss policies around bring your own device.

The first proposition posited that company policies are put in place to drive basic hygiene behaviour – good behaviours. Protecting information, internet behaviour and email uses were the most prominent references and dominant themes followed by password management, incident reporting and mobile computing. The least discussed theme was social media use.

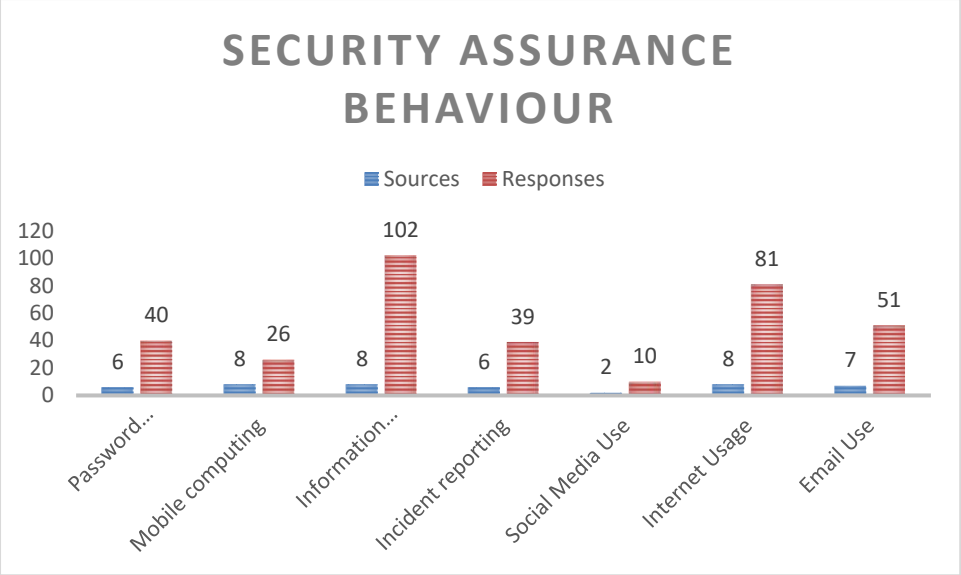


Figure 11 summary of identified behaviours in the office environment.

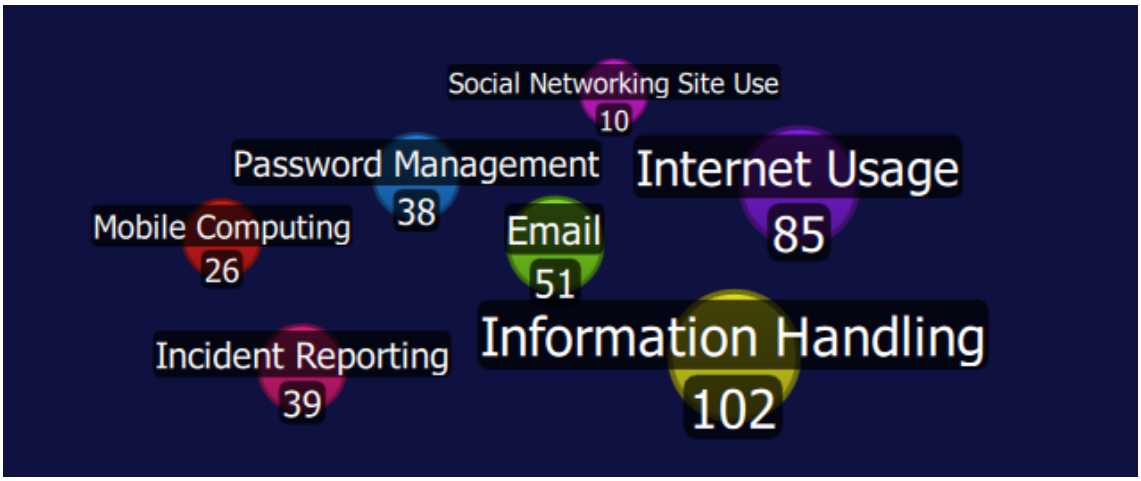


Figure 12: thematic analysis snapshot from the coding tool Quirkos

4.1.1 *Password Management*

Password Management subthemes emerged from 38 references by 6 of the 8 participants. Using strong passwords, constantly changing passwords and never sharing passwords were regarded as basic hygiene behaviours.

"*Awareness is just to let people know, but then you could use that same information if you make somebody aware and say 8 characters, multi*

alphanumeric and then later on tested a person on that question" **Participant D what constitutes a strong password.**

"You literally don't share passwords with anybody." **Participant KM on sharing of passwords**

"[…] always change your password whether you're technical or not. If you are a normal user, you've got 90 days. If you are technical, you've got 30 days." **Participant KM on changing passwords**

4.1.2 *Information Handling*

The subthemes that emerged from information handling were not inserting removable devices (such as USB's and DVD's), locking screens, not forwarding work-related information to personal email. Information Handling had the highest number of references with 102 coming from the 8 participants.

"*So, with the lockdown of USB. We have done that already and the control of that. We won't allow people.*" **Participant A on removable media and the technical control to enforce it.**

"You already know if I was in the office and I didn't lock my ***screen****, I would find my* ***screen*** *upside down"* **Participant D on locking the screen.**

"You have to motivate why you're sending data with an Excel spreadsheet attached to your Gmail address." **Participant KM on sending company information to personal email.**

4.1.3 *Email Use*

The main subthemes that emerged from Email Use were focused on reducing phishing attacks. Never open email attachments and clicking on links from unknown sources were highlighted as good behaviours.

"There's going to be obvious mistakes, there's going to be obvious, glaring mistakes sometimes not so glaring mistakes. We send it out to the whole organization and see who's going to report it and see who's going to click on

the link and we collect the data, so that's how we check compliance" **Participant KM on clicking on links.**

"We have to update our security policies such that if you know looking at the score of the email itself using our controls that are already in place for email security. Looking at the body of the email, the attachment and so on." **Participant B on how attachments are handled.**

4.1.4 *Mobile computing*

The main subthemes for mobile computing focused on incidences where personal computers were taken out of the office environment. Always Using a VPN, not connecting to public Wi-Fi to do work and not sharing a laptop with family or friends were regarded as security assuring behaviours.

"[…] so we don't want them to use their personal router because obviously we are using the VPN. If they are using their personal, we still have to think about the data." ***Participant SL on use of VPN when connecting to home router given that all their employees were given a working router.***

"All these policies that we put in place like you cannot take your PC and connect on a public Wi-Fi" **Participant SL on Wi-Fi usage.**

"The major problem we had is people's children needed to connect initially to school and we had people asking us some strange questions. It's hard to help the kids on there because our machines are locked down" **Participant A on sharing a laptop with family members.**

4.1.5 *Social networking sites (SNS) use*

The main subthemes for social networking site use focused emerged from 2 participants and had the lowest number of references with 10. Depending on the role, social media use is not allowed during work hours with the exception being departments such as marketing.

"Remember with us with the bank all social sites are closed. So no one who's got it in." **Participant SL on social media use.**

4.1.6 *Incident reporting*

The main subthemes for incident reporting emerged from 6 participants and had 36 references. Reporting security incidents to help the cybersecurity team respond quickly was regarded as basic hygiene behaviour.

"We had a team of maybe 40 people managing an environment with 30,000 people. So, you will miss stuff. So, in my opinion, you got to include people in it because they can see. You're expecting people to give you the heads up and certain conditions happen for you to respond quickly." **Participant A on reporting security incidents.**

"So you know that if the CEO plugs in a USB after I've said that no USB is plugged, then you can take the same measures and take him to HR and say this person failed to comply." **Participant KM on reporting security incidents**

4.1.7 *Internet use*

The subthemes for internet use emerged from 81 references by 6 of the 8 participants. Avoiding dubious websites and streaming sites (including YouTube) are regarded as security assuring behaviours.

"[…]so it was never blocked initially, but then we realised that even the Internet speed used to get affected in the office only because when you are streaming, people never change the quality of their videos cause then automatically on Dstv Now the videos are in HD." **Participant D on streaming sites being blocked**

"For example, if I could dive into it, like say you were browsing an adult content site on your workstation, we know that is not in line with the acceptable usage policy." **Participant PS on accessing dubious websites.**

Each focal area and their sub-themes are summarised below in Figure 13.

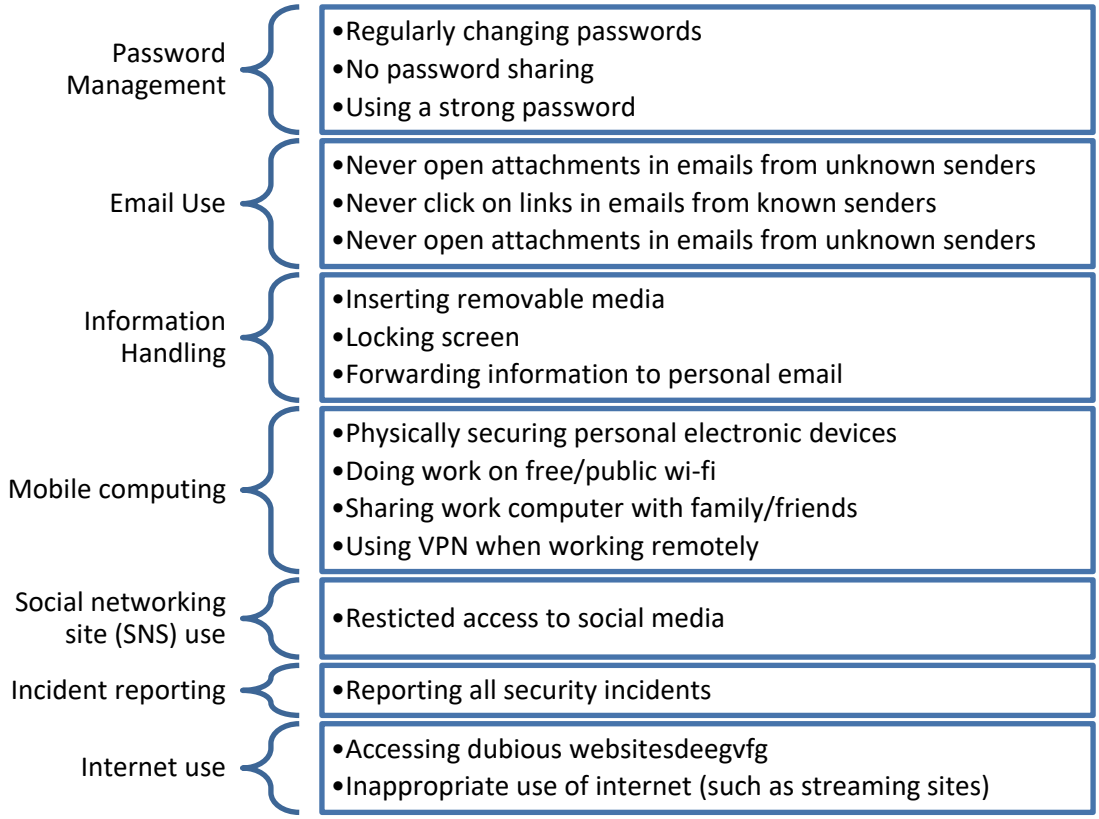


Figure 13: summary of behaviours enforced in the workplace

4.2 Results pertaining to Proposition 2

The second research objective was to uncover whether the behaviours in the workplace were transferred to the remote working environment. The second proposition argued that naïve mistakes will increase in the work remote work environment.

To identify behaviours transferred to the remote workplace, participants were asked to discuss cybersecurity behaviour changes they have noticed. All participants highlighted that there have been no significant cybersecurity behaviour changes and employees are adhering to cybersecurity policies as they did in the office environment.

Despite initially stating little to no changes that there have been little changes – with most crediting their training initiatives and technology controls – they

mentioned minor changes that were summarised in Table 4 below. Participants made 62 references regarding changes in cybersecurity behaviours which are summarised to show that not all behaviours were carried to the remote work environment.

Mobile computing emerged as the most referenced cybersecurity behaviour change. Employees were provided with devices to take home with the condition that they will be used for work purposes only. The data showed employees increasingly showed signs of using a work computer for personal reasons.

"The major problem we had is people's children needed to connect initially to school and we had people asking us some strange questions." **Participant A**

"At work, it's different, for instance at home now it's not only the employees that can have access to that computer call mom your family can have access to that computer, but your children can also have access to that computer, even a friend can come into your house and access your computer" **Participant SL**

VPN emerged as a critical tool provided to employees in order to access company information. There were however references to employees bypassing it or avoiding using it unless necessary.

"People felt like it was a huge inconvenience to log onto the VPN in order to access your emails" **Participant T**

"So what some people would do is they connect to the VPN, take the documents they want to put them on the desktop, disconnect VPN, work, work, work, work, update at the end, copy them back connect VPN then they paste them back, but they did that so that they can also do other things while they were working" **Participant D**

Information Handling emerged as another subtheme of behaviours that were not carried to the remote working environment. Printing was an essential part of certain job functions but given the lockdown on plugging removable media, which included USB devices, employees were sending information to their personal devices to complete the tasks.

"So people start distributing things a lot to their personal Gmail accounts so they can do certain things. If I'm not able to connect my laptop to a printer, I'm going to send to a personal laptop or send via Gmail" **Participant T**

Table 4: Summary of cybersecurity behaviours carried to the remote work environment

Themes	Sub-themes	Example reference
Information handling	Non-confidential information is being shared on WhatsApp	"People have shared some files over WhatsApp. There's still always that consciousness if we don't share confidential stuff over WhatsApp, we don't share confidential stuff over any non-company approved platform" Participant T
Internet Usage	Sending documents to personal email accounts to print	"So people start distributing things a lot to their personal Gmail accounts so they can do certain things. If I'm not able to connect my laptop to a printer, I'm going to send to a personal laptop or send via Gmail" Participant T
Mobile Computing	Using work computer for personal use	"The major problem we had is people's children needed to connect initially to school and we had people asking us some strange questions." Participant A
Mobile Computing	Bypassing VPN	"People felt like it was a huge inconvenience to log onto the VPN in order to access your emails" Participant T
Mobile Computing	Not locking screens in the	"I tend to leave my laptop unlocked to the extent that sometimes I would go for this walk that I have gone for

	home environment	now and I would get back and I'd find the screen locked and it goes to screensaver" Participant T

Table 4: summary of changes in cybersecurity behaviour in the remote work environment

4.3 Results pertaining to Proposition 3

The next objective of the research was to uncover which factors influence cybersecurity behaviours of remote working employees. To achieve, data was collected using a survey questionnaire answered by employees in the financial services sector – referred to as end-users. It was hypothesized that organisation factors, employee attitudes, social influence and sense of control influence complaint behaviour. For this question, both quantitative and qualitative data were collected, analysed separately. The merging will take place in the discussion section.

Descriptive Analysis of the Study Variables

To create scale elements and composite scales, descriptive statistics were developed to generate employee attitude scores. Perceptions of remote working employees desire to follow an organization's cybersecurity policies and procedures were presented as questions to answer on a 5-point Likert scale, with 1 indicating strong disagreement and 5 indicating strong agreement.

4.3.1 *Intent*

Respondents indicated a positive view of the function of policies put in place to protect the organisation when employees work remotely. This was to assess their intent to follow cybersecurity policies which is a prediction of behaviour.

Item	Variable	Mean	STD

1	When working remotely, I intend to continue complying with cybersecurity policies that I usually follow when working in the office.	4.39	0.87

4.3.2 *Personal Attitude Scale*

The personal attitude scale measured employee attitudes towards cybersecurity behaviour. six items were used to measure employee attitudes on a 5-point Likert-type scale format ranging from 1 = strongly disagree to 5 = strongly agree. Items in this scale were majority reverse-scored apart from item 1. For this section, the scores are summarised in Figure 14 below. The highest score was item 1 (*M = 4.45, somewhat agree*), the belief that there is a risk with remote working, followed by items 4 and 6 (*M = 4.39 and M = 4.39*) respectively and item 3 (*M = 4.38, somewhat agree*). Item 4 measured attitude towards risks that comes with remote working and item 6 measured attitude towards following cybersecurity measures when working remotely. Items 2 and 3 were the lowest scoring items on the personal attitude scale (*M = 3.91).*

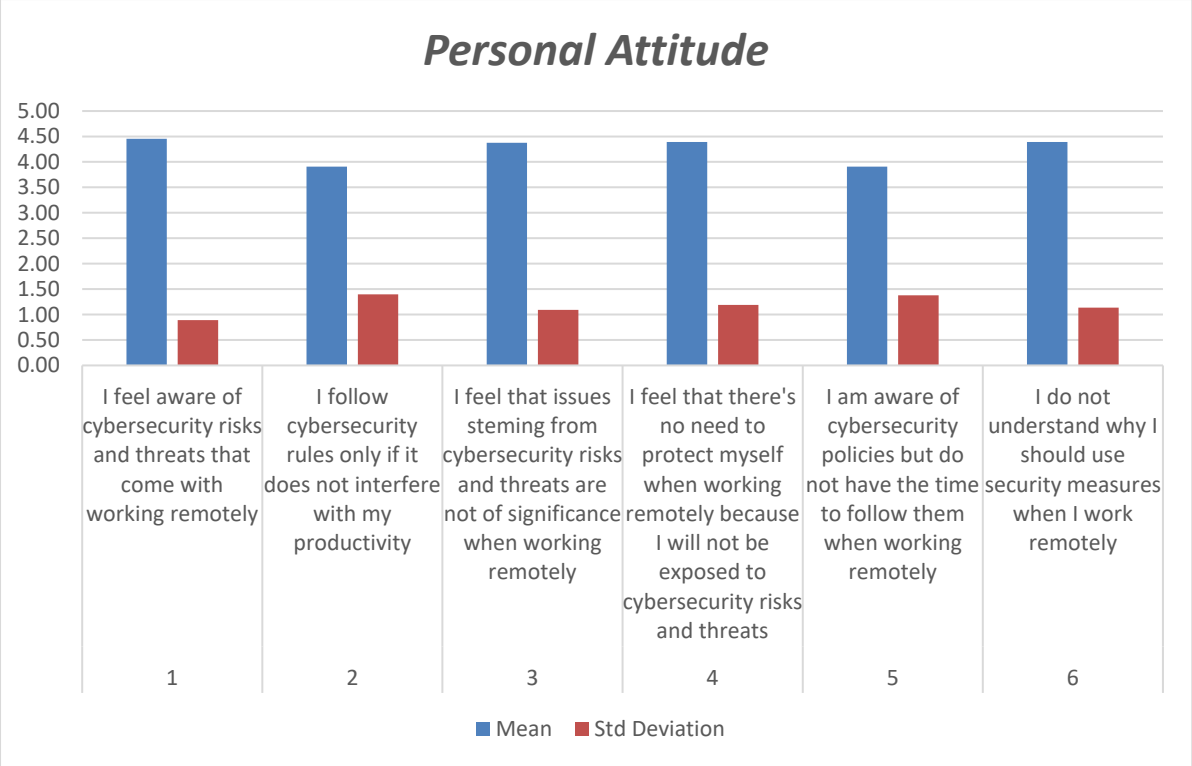


Figure 14: Descriptive analysis of Personal Attitude

Multiple regression was performed on each of the scores to evaluate the association between items on the Personal Attitude Scale and intent to comply with organisational cybersecurity policies. The hypothesis was presented as follows,

$H1_0$: There is no relationship between personal attitude and remote worker's intent to comply with cybersecurity policies.

$H1_a$: There is a relationship between personal attitude and remote worker's intent to comply with cybersecurity policies.

Several relationships were statistically significant, although they were weak. Despite being deemed statistically significant due to the limited sample size, no substantial relationship between intent to comply with cybersecurity policies (dependent variable) and several Personal Attitude Scale items were discovered, adjusted r =0.135 (this is summarised in Table 5).

Therefore, the null hypothesis was rejected at level .05 since the p-value is < 0.05 (P = 0.025). meaning there is a relationship.

Table 5 Personal Attitude Regression Analysis

Item	Variable	Standard Error	t Stat	P-value
1	*I feel aware of cybersecurity risks and threats that come with working remotely*	0.125	1.713	0.092
2	*I follow cybersecurity rules only if it does not interfere with my productivity*	0.131	0.406	0.686
3	*I feel that issues stemming from cybersecurity risks and threats are not of significance when working remotely*	0.159	0.814	0.419
4	*I feel that there's no need to protect myself when working remotely because I will not be exposed to cybersecurity risks and threats*	0.116	-0.824	0.414
5	*I am aware of cybersecurity policies but do not have the time to follow them when working remotely*	0.129	0.758	0.452
6	*I do not understand why I should use security measures when I work remotely*	0.128	0.530	0.598

4.3.3 *Social Influence*

Five items were used to formulate the Social Influence Scale composite score. This section focused on the influence of their social environment on their cybersecurity behaviours when remote working. Participants answered on a 5-point Likert-type scale, with 1 indicating strongly disagree and 5 indicating strongly agree. (this is summarised in Figure 15). Item 3, the influence of hearing about cybersecurity incidents was the highest score (*M = 4.50 somewhat agree*). The following scores were item 2, family and friends' expectation and item 4 mass media expectation both followed with *M = 3.61, neutral*. The lowest score was the influence of family and friends *M = 2.84 somewhat disagree.*

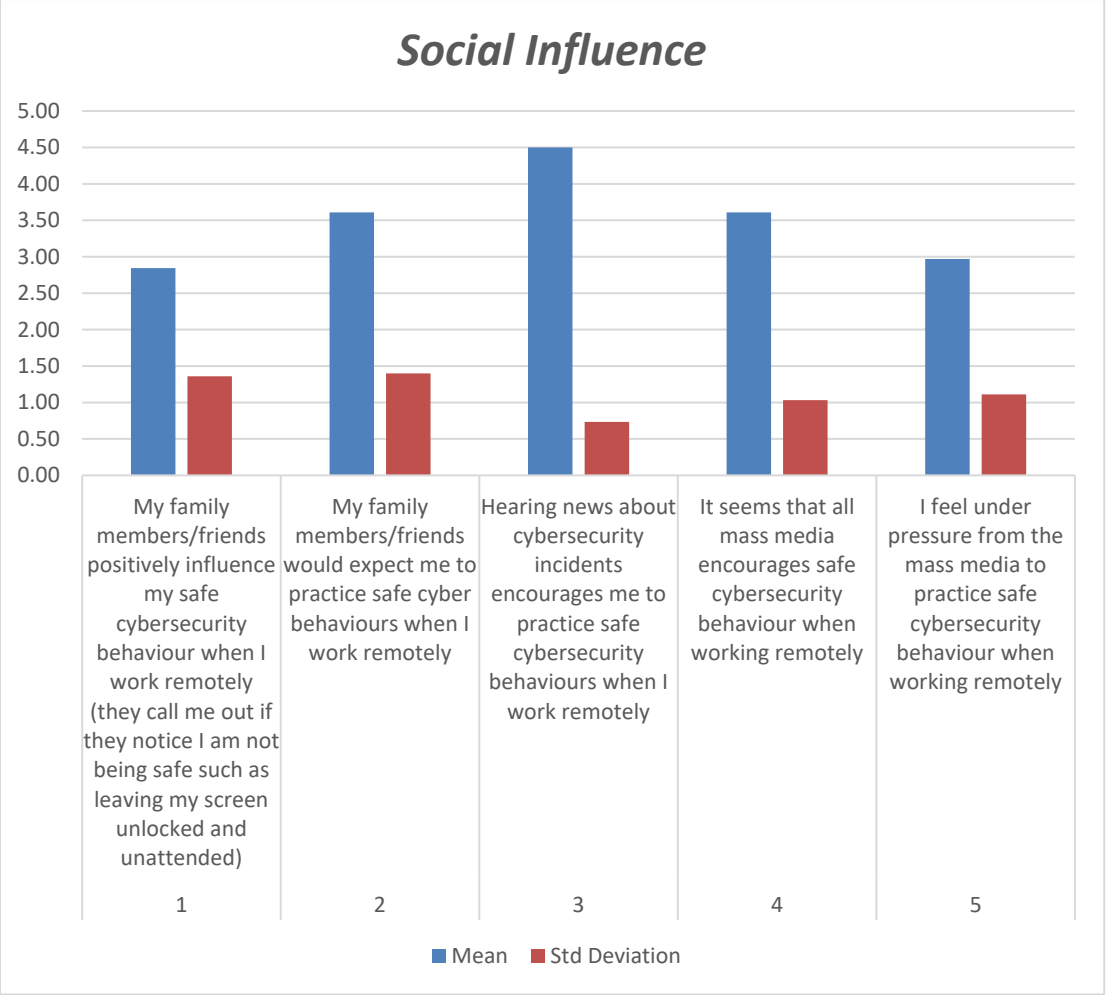


Figure 15: Descriptive analysis of Social Influence

To examine the relationship between social influences and remote workers' intent to comply with organisation cybersecurity policies, multiple regression was done on each of the items of the scale. The hypothesis was presented as follows - this is summarised in Table 6,

$H2_0$: There is no relationship between personal attitude and remote worker's intent to comply with cybersecurity policies.

$H2_a$: There is a relationship between personal attitude and remote worker's intent to comply with cybersecurity policies.

Several relationships were statistically significant, albeit weakly. Despite being deemed statistically significant limited by small sample size, no substantial relationship between intent to comply with cybersecurity regulations

(dependent variable) and the Social Influence components were discovered, adjusted *r* =. 0.086

Therefore, the null hypothesis was not rejected at level 0.05 since the p-value is > 0.05 (P = 0.067), meaning there is no relationship.

Table 6: Social Influence Regression Analysis

Item	Variable	Standard Error	t Stat	P-value
1	*My family members/friends positively influence my safe cybersecurity behaviour when I work remotely (they call me out if they notice I am not being safe such as leaving my screen unlocked and unattended)*	0.098	1.163	0.250
2	*My family members/friends would expect me to practice safe cyber behaviours when I work remotely*	0.098	0.537	0.594
3	*Hearing news about cybersecurity incidents encourages me to practice safe cybersecurity behaviours when I work remotely*	0.145	1.263	0.212
4	*It seems that all mass media encourages safe cybersecurity behaviour when working remotely*	0.115	1.362	0.178
5	*I feel under pressure from the mass media to practice safe cybersecurity behaviour when working remotely*	0.099	-0.447	0.657

4.3.4 *Sense of control*

Five questions made up the sense of control scale composite score to uncover remote working employees' belief that they are capable and in control of adhering to cybersecurity policies – this is summarised in Figure 16. The respondents answer on a five-point scale format ranging from 1 = strongly disagree to 5 = highly agreed. Item 2, measuring employee belief that complying with cybersecurity policies is easy, was the highest score (*M = 4.14, somewhat agree*). This was followed by Item 2, *Complying with cybersecurity policies is entirely under my control* (*M = 4.14, somewhat agree*) and item 4, *I believe that I am at risk of becoming a victim of a cybersecurity incident* (*M = 3.33, somewhat agree*). The lowest scores were items 4 (*M = 2.98, neutral*), *I believe that it is likely that I will become a victim of a cybersecurity incident* and

item 5 (*M = 2.05, somewhat disagree*), *I feel that it is my responsibility to protect myself from cybersecurity risks and threats when working remotely.*

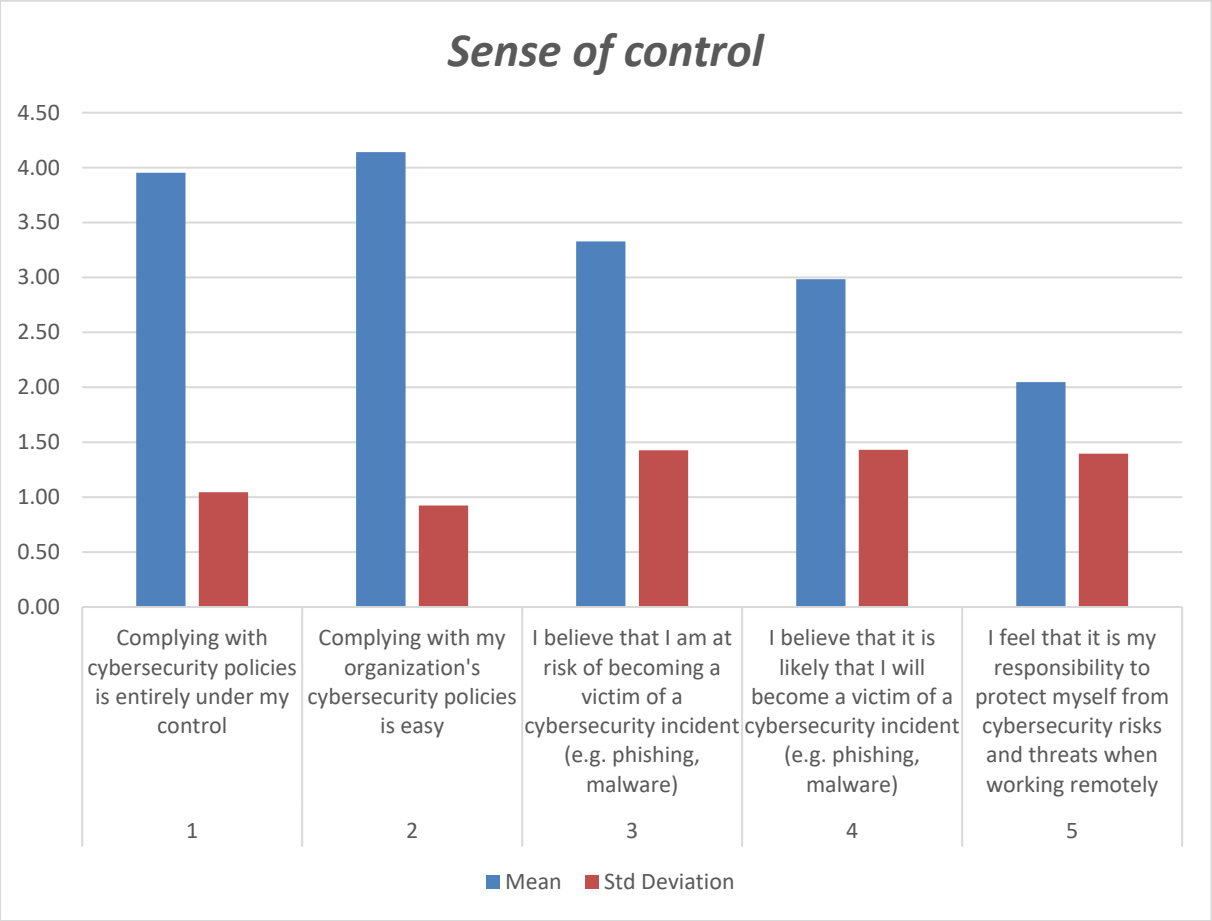


Figure 16: Descriptive analysis of Sense of Control

To examine the relationship between sense of control and remote workers' intent to comply with organisation cybersecurity policies, multiple regression was done on each of the items of the scale. The hypothesis was presented as follows,

$H3_0$: There is no relationship between sense of control and remote worker's intent to comply with cybersecurity policies.

$H3_a$: There is a relationship between sense of control and remote worker's intent to comply with cybersecurity policies.

Several relationships were statistically significant - this is summarised in Table 7), although they were weak. No meaningful link was found between intent to comply with cybersecurity policies (dependent variable) and the Sense of Control component, adjusted *r = 0.191*

Therefore, the null hypothesis was rejected at level .05 since the p-value is < 0.05 (*P = 0.004*), meaning there is a relationship.

Table 7: Sense of Control Regression Analysis

Item	Variable	Standard Error	t Stat	P-value
1	*Complying with cybersecurity policies is entirely under my control*	0.104	1.919	0.060
2	*Complying with my organization's cybersecurity policies is easy*	0.077	-0.359	0.721
3	*I believe that I am at risk of becoming a victim of a cybersecurity incident (e.g. phishing, malware)*	0.125	2.506	0.015
4	*I believe that it is likely that I will become a victim of a cybersecurity incident (e.g. phishing, malware)*	0.075	-0.644	0.522
5	*I feel that it is my responsibility to protect myself from cybersecurity risks and threats when working remotely*	0.079	0.440	0.662

4.3.5 *Organisational Factors*

Four items were used to formulate the sense of organisation factors scale to uncover the influence of organisational measures on employee intent to follow cybersecurity policies when working remotely (this is summarised in Figure 17). Item 4 (*M = 4.05, somewhat agree*), *My organization disciplines employees who violate cybersecurity policies* was the highest score followed by item 1 (*M = 3.98, somewhat agree*) and item 2 (*M = 3.88, somewhat agree*). The lowest score was item 2 (*M = 3.88, somewhat agree*), *My organization provides training to help employees improve their cybersecurity policy knowledge.*

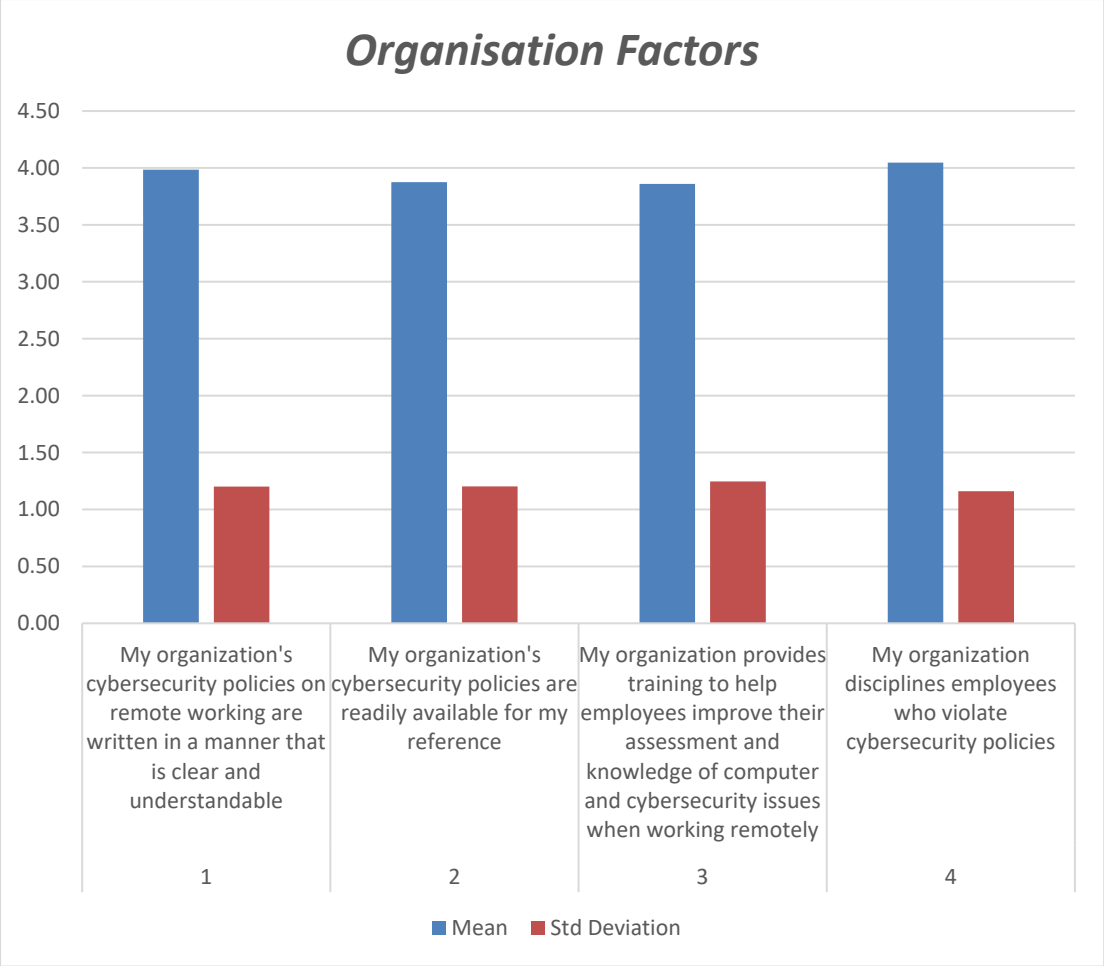


Figure 17: Descriptive analysis of Organisation Factors

Multiple regression was performed on each of the scale items to evaluate the link between organisational variables and remote workers' intent to adhere to organisational cybersecurity rules. The hypothesis was presented as follows,

$H4_0$: There is no relationship organisation factors and remote worker's intent to comply with cybersecurity policies.

$H4_a$: There is a relationship between organisation factors and remote worker's intent to comply with cybersecurity policies.

Several relationships were statistically significant, although they were weak. Despite being declared statistically significant due to the small sample size, no meaningful link was found between intent to comply with cybersecurity policies (dependent variable) and the Sense of Control component, adjusted $r = 0.050$ - this is summarised in Table 8.

Therefore, the null hypothesis was not rejected at level .05 since the p-value is > 0.05 (P = 0.136), meaning there is a relationship between organisation factors and remote worker's intent to comply with cybersecurity policies.

Table 8: Organisation Factors Regression Analysis

Item	Variable	Standard Error	t Stat	P-value
1	*My organization's cybersecurity policies on remote working are written in a manner that is clear and understandable*	0.152828	0.06338	0.949678
2	*My organization's cybersecurity policies are readily available for my reference*	0.151899	0.742633	0.460651
3	*My organization provides training to help employees improve their assessment and knowledge of computer and cybersecurity issues when working remotely*	0.131718	0.143606	0.886301
4	*My organization disciplines employees who violate cybersecurity policies*	0.124403	1.08385	0.282841

4.4 Summary of the results/findings

The findings identified basic hygiene behaviours with information handling being the most referenced. The least referenced was social media use. The results also highlighted the behaviours carried to the remote environment. This showed that mobile computing was the most impacted behaviour as employees prioritised their productivity, which leads to naïve mistakes.

Results from multiple regression analysis highlighted which behaviours had the most influence on intent to comply with cybersecurity policies. Although weak, several relationships were statistically significant. Despite being deemed statistically significant due to the limited sample size, no substantial relationship between intent to comply with cybersecurity policies (dependent variable) and several items on the several Personal Attitude, Social Influence, Sense of Control and Organisation Factors scales.

CHAPTER 5. DISCUSSION OF THE RESULTS OR FINDINGS

Introduction

The previous, Chapter 4, presented the findings from the qualitative and quantitative data collected. The qualitative data stemmed from semi-structured interviews with cybersecurity professionals in the financial services sector who are responsible for enforcing cybersecurity behaviours that reduces cybersecurity risk. Thematic analysis was employed to identify key themes from the interview. The quantitative data stemmed from a survey questionnaire that was answered by employees in the financial services sector – also referred to as end-users. The purpose of this chapter is to discuss the results from the previous chapter in relation to the literature identified in chapter 2 and the research questions identified in chapter 1.

5.1 Discussion pertaining to Proposition 1

The first research question was to identify the behaviours enforced in the office environment. The first position posited that financial services organisations enforce basic hygiene behaviours to supplement technical controls. The HAIS-Q, which consists of seven focal areas that include Internet Use (IU), Mobile Devices (MD), Password Management (PM), Email Use (EU), Social Media Use (SMU), Information Handling (IH), and Incident Reporting (IR) was used as a guide to identify and group these behaviours. Various aspects of each focal area were mentioned by all the participants. It is imperative to note that these results were not surprising given that they focus on strategic areas that humans pause a threat, whether this is intentional or unintentional (Leonard et al., 2004). The focus areas of the HAIS-Q are sources of cybersecurity behaviours that expose organisations to cyberthreats. This is in line with the literature that organisations will focus on basic hygiene cybersecurity behaviours (Alqahtani, 2017). These behaviours were further analysed to identify behaviours under each focal area.

Using strong passwords, constantly changing passwords, and never sharing passwords were regarded as basic hygiene behaviours for Password Management. These were in line with the findings based on an analysis of cybersecurity policies and identified that locking workstations, never sharing passwords and choosing a strong password as good security behaviour. Literature highlights passwords as an essential component of many security solutions, often used as the first line of defence (Zheng, Cheng, Zhang, Zhao, & Wang, 2018). To ensure that passwords – in addition to security control – serve the function of being the first line of defence, companies set rules to drive password behaviour (Sohrabi Safa et al., 2016). These include password length, complexity and change frequency (Blythe, Coventry, & Little, 2015b; Shropshire, Warkentin, & Sharma, 2015).

Information handling which was the most referenced behaviour had never inserting removable devices (such as USB devices), locking the screen, not forwarding work-related information to personal email as good behaviours. This is consistent with findings by Pattinson et al. (2015) which highlighted disposing of sensitive documents, not inserting DVDs/USB devices, leaving sensitive material secured as good behaviours.

Never opening emails, attachments and clicking on links from unknown sources emerged as good email usage behaviours. Employees need to be aware of increased attempts in Covid 19 related scams (Furnell & Shah, 2020) and practising good email usage behaviours is an important element of reducing the chances of successful phishing attempts. Email usage is a critical aspect of cybersecurity behaviours that businesses enforce (Parsons et al., 2014). The results correspond with literature whereby not opening attachments (Alohali, Clarke, Furnell, & Albakri, 2017; Blythe et al., 2015b; Pattinson et al., 2015) as well as not opening and clicking on an email from unknown senders (Bélanger, Collignon, Enget, & Negangard, 2017; Safa et al., 2015; Shropshire et al., 2015) regarded as good email usage behaviour.

Mobile computing behaviours focus on securing devices with work information outside the company premises (Gangire et al., 2020). Not connecting to public Wi-Fi to do work and not sharing a laptop with family or friends were emerged

as good security behaviour. The themes are consistent with literature whereby physically securing mobile devices, sending sensitive information via public Wi-Fi and guarding against shoulder surfing (Bauer et al., 2017; Curry et al., 2018). Our data highlighted the use of VPN as an integral part of remote working measures that companies put in place. This was not to be found in the analysed literature by (Parsons et al., 2014).

Avoiding dubious websites and streaming sites (including YouTube) emerged as good internet usage behaviours. (Safa et al., 2015) highlighted that hackers have become creative in their approach to installing viruses by creating websites that offer free downloads. Avoiding dubious websites that offer free downloads as well as downloading software is regarded as good internet behaviour. One of the participants highlighted that streaming website such as Netflix and Dstv Now have recently been added as restricted sites, highlighting behaviour that should be investigated further.

Incident reporting enables the company security teams to respond to issues that may increase cybersecurity risk (Blythe et al., 2015b). Reporting all cybersecurity incidents that increases risk emerged as good behaviour. This was consistent with (Parsons et al., 2014) who found incident reporting to be an integral part of behaviours companies enforce.

Social Media was the least referenced cybersecurity behaviour. Bélanger et al. (2017) highlighted avoiding social networking websites during work hours as good cybersecurity behaviour. This is in correspondence with the subtheme that emerged from the data. Social media usage was highlighted to be the least important element from the thematic analysis which could highlight that organisation no not give it as much intention as the other highlighted behaviours. This was surprising because

5.2 Discussions pertaining to Proposition 2

The second research objective was to uncover whether the behaviours in the workplace were transferred to the remote working environment. The second proposition argued that naïve mistakes will increase in the work remote work

environment. Naïve mistakes are accidental behaviours from employees that could increase the cybersecurity risk of an organisation (Stanton et al., 2005). To identify behaviours transferred to the remote workplace, participants were asked to discuss cybersecurity behaviour changes they have noticed. Findings suggest that employees were adhering to cybersecurity policies but when behaviours are isolated, naïve mistakes were present. Participants made 62 references regarding changes in cybersecurity behaviours which are summarised to show that not all behaviours were carried to the remote work environment.

Not using work-issued devices for personal use was one of the good basic hygiene behaviours. The research data showed that the boundaries were blurred in the remote working environment, increasing the chances of work-issued devices and leading to naïve mistakes. Employees started engaging in using work/issued devices for personal use such as asking if their family members can make use of their work devices. The intent is not malicious, but the behaviour can have negative consequences.

Results showed that remote working had a positive influence on productivity because employee work/life balance improved. Organisational psychology highlights that increased work/balance blurs the boundary between work and personal activities (Blythe et al., 2015), leading to work-issued devices being used for personal needs. The argument is that employees find quickly using your work-issued for a personal need – for example, quickly shopping online – is more convenient than stepping away from a work-issued device to quickly log into a personal device. There is also a sense of fear that other members will question them should they not answer their enterprise communication application such as Microsoft Teams.

Researchers have found that employees with low work/life balance have a higher propensity to reduce the boundaries between work and personal life duties. As a result, they are more likely to engage in naïve or accidental cybersecurity behaviour. This study's results showed increased work/life balance, however, employees showed signs of using work computers for personal needs. (Blythe et al., 2015b) found that employees with reduced

remote working were less likely to use their work/issued devices for work purposes and argued that remote working has a positive influence on naïve mobile computing mistakes. This is interesting to note that data from the quantitative results taken from end-users showed friends or family members had a neutral influence – mean rating of 2.84, somewhat disagree – on their cybersecurity behaviour. Highlighting that productivity takes preference first because that is what employees are measured on. This interesting to note the different views between cybersecurity professionals and end-users.

This was evident in the next category of cybersecurity behaviours not carried to the work remote environment. VPN emerged as a critical tool provided to employees to access company information. There were however references to employees bypassing it or avoiding using it unless necessary.

What was interesting from this data was that cybersecurity professionals who were aware of this happening did not mention possible solutions. This could be because employees are scared to speak up or their feedback is not taken into consideration. Sometimes employees are an organization's first line of defence and can provide valuable insights into how companies can improve their cybersecurity measures but this is not always taken seriously (Kirlappos et al., 2014).

Information Handling emerged as another subtheme of behaviours that were not carried to the remote working environment. Printing was an essential part of certain job functions but given the lockdown on plugging removable media, which included USB devices, employees were sending information to their personal devices to complete the tasks. Job performance once again prevailed over cybersecurity behaviours that end-users acknowledge as risky behaviour.

It was interesting to note that financial services companies did not permit Bring Your Own Device – despite phones being used for two-factor authentication – to reduce the likelihood of work devices being used for personal needs. This method has been effective for some behaviours but other not others. It is evident that employees have continued to comply and behave securely but when secure behaviour impedes their productivity, employees will bypass

security measures. The data showed that the intention behind the changes in behaviours was not malicious but could have negative consequences for the organisation.

5.3 Discussion pertaining to Hypothesis 1

The next objective to uncover which factors influence cybersecurity behaviours of remote working employees. The hypothesis posited that employee sense of control and organisation factors (training and awareness) would positively influence their behaviours towards adhering to cybersecurity policies. This research sub-question was answered employing descriptive and inferential analysis using a modified theory of planned behaviour questionnaire that addressed organisational variables.

5.3.1 *Intent*

Remote working employees indicated that they were willing to comply with their company policies when working remotely (*M* = 4.39 on a scale from 1 = *strongly disagree* to 5 = *strongly agree*).

5.3.2 *Personal Attitude*

a. *Quantitative Data*

Multiple regression was conducted on each of the scale's items to evaluate the association between items on the Personal Attitude Scale and intention to adhere with organisational cybersecurity policies. The hypothesis was presented as follows,

H1o: There is no relationship between personal attitude and remote worker's intent to comply with cybersecurity policies.

H1a: There is a relationship between personal attitude and remote worker's intent to comply with cybersecurity policies.

Remote working employees indicated that they recognise the value of cybersecurity policies, according to their responses to Personal Attitude items. Remote working employees indicated a strong belief (strongly agree, M = 4.45) that they feel aware of cybersecurity risks and threats that come with remote working (item 1), understand that they need to behave safely *(item 4 and 6 = M 4.39)* and would make time to comply with policies even when at the sacrifice of productivity *(items 2 and 5 = M 3.91)*.

Kirlappos et al., (2014) highlighted employees' real policy compliance intentions are largely influenced by their personal views or attitude. The results of this study found that intrinsic factors did have a significant influence on remote workers' intentions to follow security measures, thus complying with cybersecurity policies. The finding of this section contradicted Herath & Rao's 2009 study. Overall *(composite score average, M = 4.24)*, remote workers indicated that they somewhat agree that personal attitude influences cybersecurity behaviour. The hypothesis results showed that there was sufficient evidence to conclude there is a significant linear relationship between personal attitude and intent to comply with cybersecurity. Therefore, the null hypothesis was rejected at level 0.05 since the p-value is < 0.05 (P = 0.025).

b. *Qualitative Data*

As discussed in the methodology section of the research paper – chapter 3 – the mixing of the qualitative and quantitative elements would occur in the discussion section. Using the qualitative data, insights about factors that influence cybersecurity behaviours was used to provide deeper meaning from the quantitative data (Bryman, 2006). Themes emerging from qualitative results showed that attitudes towards cybersecurity behaviour do not always equate to the actual behaviour. Respondents highlighted that employee generally comply with cybersecurity policies despite seeing not always have a favourable attitude towards it. Firstly, employees perceive cybersecurity to be an IT problem.

Secondly, employees perceive the process of adhering to cybersecurity measures as an inconvenience and hindrance to their productivity. (Kirlappos

et al., 2014) found that when processes to comply become cumbersome or unreasonable, humans make mistakes or stop complying. The resulting frustration develops a poor attitude towards cybersecurity, which negatively impacts the success of awareness and education efforts companies implement - even measures with little impact on productivity (Albrechtsen & Hovden, 2009). The disparity stems from the belief that cybersecurity compliance is binary - employees either comply or do not comply due to a lack of understanding. The data is in line with (Kirlappos et al., 2014)'s argument that cybersecurity professionals attribute policy noncompliance to lack of awareness.

When assessing attitude and compliant behaviour, organisations fail to consider the requirements of the business, the context and the environment in which interaction between human technology (Faily, 2018). Therefore, personal attitude's influence on actual behaviour is mediated by job requirements – often ignored by the cybersecurity function.

5.3.3 *Social influence Scale*

a. *Quantitative Data*

To examine the relationship between social influences and remote workers' intent to comply with organisation cybersecurity policies, multiple regression was done on each of the items of the scale. The hypothesis was presented as follows,

H2o: There is no relationship between social influences and remote worker's intent to comply with cybersecurity policies.

H2a: There is a relationship between social influences and remote worker's intent to comply with cybersecurity policies.

The highest mean rating for social influence was 4.50 (strongly agree) for item 3, the influence of hearing news about cybersecurity incidents on their inclination to follow cybersecurity policies when working remotely. They were

subsequently neutral on whether families/friends would expect them to behave safely in the remote cybersecurity space. The lowest mean rating was 2.84 (somewhat disagree) that their friends/family members influenced their cybersecurity behaviour when working remotely. Remote working employees were neutral on mass media's impact on encouraging safer cybersecurity behaviour (item 4, M = 3.61). In addition, they were also neutral (M = 2.97) on feeling a sense of pressure from mass media to behave safely in the remote working environment.

(2009) found subjective norm – acting as a result of another peers' behaviour – to positively influence compliant behaviour in the work environment. This study did not find a similar theme when focusing on the remote working environment. In the remote environment, employees have reduced interaction with their peers which and increase their interaction with family and friends. It has been empirically demonstrated that family members and friends have a substantial impact on users' intent to behave safely (B.-Y. Ng & Rahim, 2005). Like Haeussinger & Kranz (2013) results in this study showed that family and friend's influence was neutral or not significant. Hearing news about cybersecurity incidents was the most important influencer of compliant behaviour. This was not in line with Ng and Rahim (2005) finding that mass media, along with family, influence important factors that influence a remote worker user's intention to comply with cybersecurity policies.

Overall (composite score average, M = 3.51), remote workers indicated that social influence's influence was neutral. This was not surprising as previous research found that family and friends have minimal influence on cybersecurity behaviour (Simonet & Teufel, 2019). The hypothesis results showed that there was insufficient evidence to conclude there is an insignificant linear relationship between social influence and intent to comply with cybersecurity. Therefore, the null hypothesis was not rejected at level 0.05 since the p-value is > 0.05 (P = 0.067).

b. ***Qualitative Data***

Results from our qualitative data showed employee environment has positively influenced employee compliant behaviour. Cybersecurity professionals believed that employee personal environment and information obtained from outside sources like banks positively influenced their behaviour. There was no substantial motivation for this but rather an assumption. Haeussinger and Kranz (2013) also found that external sources such as government institutions influence employee compliant behaviour. Cybersecurity has influenced their personal lives, leading to compliant behaviour.

5.3.4 *Sense of Control Scale*

a. ***Quantitative Results***

To examine the relationship between sense of control and remote workers' intent to comply with organisation cybersecurity policies, multiple regression was done on each of the items of the scale. The hypothesis was presented as follows,

H3o: There is no relationship between sense of control and remote worker's intent to comply with cybersecurity policies.

H3a: There is a relationship between sense of control and remote worker's intent to comply with cybersecurity policies.

Remote workers indicated that complying with their organisation's cybersecurity policies is easy *(item 2, M = 4.14)* and that they somewhat agreed that complying with cybersecurity policies were entirely under their control (item 1, M = 3.95). Interestingly, remote workers believed that protecting themselves in the remote environment was not entirely under their control *(item 5, M = 4.14).*

According to the findings by (Spitzmüller & Stanton, 2006), organizational workers are more inclined to act on their attitudes if they believe to possess the required control and expertise to do so. Overall (composite score average, M

= 3.29), remote workers indicated that sense of control's influence was neutral. This was evident in this study and could be linked to item 2 on the organisation scale, *My organization's cybersecurity policies on remote working are written in a manner that is clear and understandable (M = 3.98),* showing that this might play an important factor.

The hypothesis results showed that there was sufficient evidence to conclude there is a significant linear relationship between sense of control and intent to comply with cybersecurity. Therefore, the null hypothesis was rejected at level 0.05 since the p-value is < 0.05 (*P = 0.004*).

b. ***Qualitative Results***

Qualitative results showed that companies relied on VPN to restrict employee access to company information resources. As a result, they started to feel less in control and devised their own workarounds.

(Kirlappos et al., 2014) found this to be evident in their study when employees ignored VPN because it slowed them down.

5.3.5 *Organisation Factors*

a. ***Quantitative Results***

To examine the relationship between organizational factors and remote workers' intent to comply with organisation cybersecurity policies, multiple regression was done on each of the items of the scale. The hypothesis was presented as follows,

H4a: There is no relationship between organizational factors and remote worker's intent to comply with cybersecurity policies.

H4a: There is no relationship between organizational factors and remote worker's intent to comply with cybersecurity policies.

The results showed that violating cybersecurity policies is a behaviour that is the most important organisation factor. Research has shown that perceived

severity – being dismissed – influences cybersecurity behaviour (Yoon & Kim, 2013). This was followed by the belief that policies on remote working were written in a manner that was clear and understandable. Should remote working employees forget or have questions about a certain behaviour, they indicated that policies were readily available and accessible for reference (item 2, M = 3.88). This was followed by a belief that their organization provides training to help them improve their knowledge of cybersecurity risks (item 3, M = 3.87).

Overall (composite score average, M = 3.94), remote workers indicated that organisation factors slightly influenced their cybersecurity behaviour. The hypothesis results showed that organisation factors influence was weak in their intention to comply with cybersecurity behaviour. Simonet & Teufel (2019) found a weak influence of organisational measures on cybersecurity behaviour which was in line with this study's result.

a. *Qualitative Results*

Qualitative results showed that organisations relied on technical controls, awareness and training to increase compliant behaviour in the remote workplace. An emergent theme from qualitative results showed remote working was not new. Respondents believed this to have influenced compliant behaviour because it was not a new concept. This was expected given that organisations primarily rely on technology solutions to enable employees to work remotely but this is not sufficient, it requires dedication and buy-in from the employees to be successful (ENISA, 2019; Kirlappos et al., 2014). The fact that remote working was experimented with before, indicates that the organisation head took key learnings from previous experience.

5.3.6 *Discussion in relation to the body of knowledge*

The findings of this study's results are consistent with Ajzen's (2005) theory of planned behaviour which argues that attitude plays a more important role than normative beliefs. Where the results of this study deviates from other research that subject norm – also known as social pressure – was not a determinant of intention. Ng and Rahim (2005) found that subjective norm was a determinant

of intention, which was more consistent with the theory of planned behaviour – it is important to note that their sample consisted of 233 home users who were not nearly remote workers. Godlove (2012) found that personal attitude was the more significant than social pressure in determining intention to comply with cybersecurity policies. This presents argument for the qualitative element's results despite its sample size. Interestingly, this research deviates from Ng and Rahim (2005) findings that perceived behavioural control to have minor significance on intention to comply. In relation to Simonet and Teufel (2019), this study's results support showed that organisation factors have minor influence on cybersecurity behaviours.

5.4 Conclusion

The results showed that organisations put in place basic hygiene behaviours to reduce cybersecurity risk – in addition to technical controls. Information handling was highlighted as the most important cybersecurity behaviour and social network site use was the least referenced.

Results indicated that there has been little change in employee behaviour in the remote environment, but some naïve mistakes increased. Mobile computing was the most affected behaviour whereby employees bypassed security measures to not lose productivity. Employees showed intention to use work devices for personal needs.

Quantitative results showed that personal attitude and sense of control had influenced compliant behaviour more than social pressure and organisational factors.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

The present study aimed to understand whether employees carry cybersecurity behaviours enforced in within company office environment to the remote workplace as well as understand which factors influence these behaviours. This chapter revisits the objective of the study to draw a conclusion based on the findings. This chapters also proposes recommendations for policymakers and future research. The Human Aspect Of Cybersecurity Questionnaire guided the theoretical framework of the research followed

6.2 Conclusions regarding research objective 1

The first proposition posited that company policies are put in place to drive security assuring behaviour – good behaviours. Protecting information, internet behaviour and email uses were the most prominent references and dominant themes followed by password management, incident reporting and mobile computing. The least discussed theme was social media use.

This study's results did not deviate from the literature, this is because financial services organisations are regulated and follow set guidelines. Responses between respondents were harmonious. The HAIS questionnaire provided a foundation to categorise cybersecurity behaviours encouraged in the workplace. This study showed however, it focused mainly on behaviours in the office environment and ignored behaviours more prevalent in the remote workplace – such as logging on to a VPN. This was in line with Kirlappos et al. (2015) argument that cybersecurity behaviours are viewed from the organisation context and ignore their feasibility in the remote environment. This presents an opportunity for measuring tools that factor in the context in which the behaviour occurs.

6.3 Conclusions regarding research objective 2

The second research objective was to uncover whether the behaviours in the workplace were transferred to the remote working environment. The second proposition argued that naïve mistakes will increase in the work remote work environment. Despite initially stating little to no changes that there have been little changes – with most crediting their training initiatives and technology controls. Mobile computing is the most influential behaviour in the remote work environment showing major changes in employee behaviour. This is partly because the between work and life becomes blurred in the remote working environment, resulting in more naive mistakes. This study found that employees exhibited increased intent to use their work given laptops for personal needs when this line was blurred but their intention was not harmful.

Adopting VPN negatively influenced employee compliance because it hindered their ability to deliver on their tasks. remote working employees viewed VPNs as an inhibitor to their productivity subsequently bypassed them in favour of delivery on their job requirement. This behaviour was not communicated back to the business for changes to be implemented nor the tools to be reviewed. This signal that employees may be scared to provide feedback or security is a priority, no matter the cost.

The results showed that not all cybersecurity behaviours enforced in the work environment on transferred when employees are working remotely. When taking a deeper look into the behaviours that are not transferred to the remote environment, this study found that only behaviours that hinder productivity are ignored in the remote environment. Because the study's aim was not to confirm or disapprove the model, there is an argument that despite identifying expected compliant behaviour, some behaviour armour relevant to the office environment and others are more relevant in the remote environment.

6.4 Conclusions regarding research objective 3

The final objective of this research was to uncover which factors influence cybersecurity behaviour - this study focused on policy compliance which is

linked to basic hygiene behaviour. Using a modified version of Ajzen's theory of planned behaviour, personal attitude, social influence, sense of control and organisational measures' influence on cybersecurity compliance were investigated. The study's quantitative (employee point of view) results showed an overall positive attitude towards cybersecurity policies and employees would take necessary steps to comply – sometimes at the cost of productivity. This study's results showed that personal attitude and sense of control had a stronger influence on employees than social influence and organisational measures. Sense of control influenced how well employees believed they could cope with complying with cybersecurity policies, most respondents agreed that complying is easy. This could indicate that employee training is equipping them to better comply with policies (Shillair, 2016) but there are other factors such as previous experience that was not investigated in this study.

Organisational measures' weak influence was also prevalent with previous studies (Rader & Wash, 2015; Shillair, 2016) but that was attributed to limited training. This study showed that employees received extensive training even when working remotely but still showed weak influence. This could be attributed to the belief that cybersecurity is part of life and it has become a habit. The other factor could be due to the industry being regulated and cross-company policies being homogeneous, leading to employees being familiar with the compliant behaviour (Tariq, 2018). Social influence's influence was shown to be weak in influencing cybersecurity behaviour despite employees agreeing that hearing from mass media affects their behaviour. External sources such as radio, the internet and television has been found to influence behaviour (Simonet & Teufel, 2019) but not significantly.

The views of employees and cybersecurity professionals on which factors influence cybersecurity behaviour seemed to contradict. Cybersecurity professionals credited to lack of BYOD, strict systems lockdown and cybersecurity training as the main driver of cybersecurity compliant behaviour. While employee responses highlighted sense of control as the main driver of compliant behaviour. This study showed organisational factors increase compliant behaviour which consequently influences sense of control.

6.5 Recommendations

From a theoretical perspective, the human aspect of the cybersecurity questionnaire provided a good measurement of employee cybersecurity behaviour. It is a tool that organisations should make use of as a litmus test to see the awareness of their employees' knowledge of cybersecurity is measures put in place. This will help them to diagnose potential risks that may be anticipated based on employee assessment. This study identified some behaviours that the questionnaire did not give attention to concerning mobile computing. Very little attention was given to VPN which was found to be an integral behaviour that influenced basic hygiene behaviour.

From the findings of this study, the following are recommendations for cybersecurity professionals:

This study showed that employees show a positive attitude towards compliant behaviour and are willing to continue to comply in the remote environment. This may be an indication that organisational initiatives put in place, such as awareness and training, in conjunction with technology measures such as not allowing BYOD are proving to be effective. the study did show that there are instances where employees do not comply with required behaviours. However, this is influenced by their task goals and job performance.

When policies are being evaluated considerable attention paid to how these measures will influence productivity or employee task objectives. This can be circumvented by including cybersecurity as part of key performance indicators which will allow employees to provide feedback to the business. Companies need to have a better understanding of employee personal and work boundaries which may help explain some behaviours that deviate from policies.

6.6 Suggestions for further research

Although the study provided a holistic understanding of cybersecurity behaviour in the workplace and the remote workplace, the quantitative element still relied on constructs that did not emerge from the qualitative element of the

research. Future research should look at this same problem from a different lens, by focusing on a sequential mixed-method strategy. Future research should also gather qualitative interviews should also be conducted with employees to get more insights. The research will benefit from a larger quantitative sample.

This research identified that employees may take corners when their job performance is at risk. This is despite being aware of the risks associated with some cybersecurity, they still executed the behaviour. Future research should explore or factor the context of job requirements on cybersecurity behaviours to uncover whether this has a major significance over other elements of the theory of planned behaviour.

Another area of research would be to focus on another industry that is not as regulated as the financial services industry to understand the role of remote working on cybersecurity behaviours. One of the reasons behind some similar themes in cybersecurity behaviours were identified in the first proposition was because cybersecurity behaviours in the financial services industry are governed by regulation. It is expected that they will follow similar guidelines. This may not be the case for other industries.

REFERENCES

Adams, A., & Sasse, M. A. (1999). USERS ARE NOT THE ENEMY : Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, *42*(12).

Ajzen, I., & Fishbein, M. (1973). Attitudinal and normative variables as predictors of specific behavior. *Journal of Personality and Social Psychology*, *27*(1), 41. Retrieved from https://psycnet.apa.org/journals/psp/27/1/41/

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476–490. doi:10.1016/j.cose.2009.01.003

Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017, July). Information security behavior: Recognizing the influencers. *2017 Computing Conference*, 844–853. doi:10.1109/SAI.2017.8252194

Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, *124*, 691–697. doi:10.1016/j.procs.2017.12.206

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *ArXiv*.

Baer, R. A., Smith, G. T., Lykins, E., Button, D., Krietemeyer, J., Sauer, S., … Williams, J. M. G. (2008). Construct validity of the five facet mindfulness questionnaire in meditating and nonmeditating samples. *Assessment*, *15*(3), 329–342. doi:10.1177/1073191107313003

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145–159. doi:10.1016/j.cose.2017.04.009

Beel, J., & Gipp, B. (2009, April). Google Scholar's ranking algorithm: The impact of citation counts (An empirical study). *2009 Third International Conference on Research Challenges in Information Science*, 439–446. doi:10.1109/RCIS.2009.5089308

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. doi:10.1016/j.im.2017.01.003

Benbasat, I. (2010). Special issue information security policy compiance an empirical study of rationality - Based beliefs. *The Mississippi Quarterly*, *34*(3).

Blythe, J. M., Coventry, L., & Little, L. (2015a). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. *Symposium on Usable Privacy and Security (SOUPS)*, *22*. Retrieved from https://core.ac.uk/download/pdf/74228707.pdf

Blythe, J. M., Coventry, L., & Little, L. (2015b). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 103–122. Retrieved from

https://www.usenix.org/system/files/conference/soups2015/soups15-paper-blythe.pdf

Bryman, A. (2006). *Mixed Methods* (A. Bryman, Ed.). doi:10.4135/9781446262566

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*, *34*(SPEC.3). doi:10.2307/25750690

Calic, D., Pattinson, M. R., Parsons, K., Butavicius, M. A., & McCormac, A. (2016). Naïve and Accidental Behaviours that Compromise Information Security: What the Experts Think. *HAISA*, 12–21. Retrieved from https://books.google.co.za/books?hl=en&lr=&id=zRqqDAAAQBAJ&oi=fnd&pg=PA12&dq=hais-q+questionnaire&ots=lu_S42DmUH&sig=IIOKaMD3vb6bkJgu-O07A16vpvc

Caputo, D. D., Pfleeger, S. L., Sasse, M. A., Ammann, P., Offutt, J., & Deng, L. (2016). Barriers to usable security? Three organizational case studies. *IEEE Security & Privacy*, *14*(5), 22–32. doi:10.1109/msp.2016.95

Collins, K. (2015). Advanced sampling designs in mixed research: Current practices and emerging trends in the social and behavioral sciences. In *SAGE Handbook of Mixed Methods in Social & Behavioral Research* (pp. 353–378). doi:10.4135/9781506335193.n15

Collins, K., Onwuegbuzie, A., & Jiao, Q. (2007). A mixed methods investigation of mixed methods sampling designs in social and health science

research. *Journal of Mixed Methods Research*, *1*(3), 267–294. doi:10.1177/1558689807299526

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10). Retrieved from https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

Creswell, J. W. (2007). Choosing a mixed methods design. In *Designing and conducting mixed methods research*.

Creswell, J. W. (2009). Qualitative, Quantitative, and Mixed Methods Approaches The Selection of a Research Design. *Research Design*.

Creswell, J. W. (2013). Steps in Conducting a Scholarly Mixed Methods Study: What I am looking for core characteristics: Do you have a quantitative database? (closed- ended). *University of Nebraska - Lincoln*.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design : Qualitative, Qualitative, Quantitative, and Mixed Methods Research Designs*.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Retrieved from https://play.google.com/store/books/details?id=DLbBDQAAQBAJ

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*(1), 90–101. doi:10.1016/j.cose.2012.09.010

Curry, M., Marshall, B., Crossler, R. E., & Correia, J. (2018). InfoSec Process Action Model (IPAM). *ACM SIGMIS Database: The DATABASE for*

Advances in Information Systems, *49*(SI), 49–66. doi:10.1145/3210530.3210535

D'Arcy, J., & Devaraj, S. (2012). Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. *Decision Sciences*, *43*(6). doi:10.1111/j.1540-5915.2012.00383.x

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1). doi:10.1287/isre.1070.0160

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*. Retrieved from https://muse.jhu.edu/article/398730/summary

Deloitte. (2020). *Remote Work The New Norm*. Retrieved from Deloitte website: https://www2.deloitte.com/content/dam/Deloitte/gh/Documents/human-capital/gh-remote-work-the-new-normal.pdf

Development and validation of instruments of information security deviant behavior. (2014). *Decision Support Systems*, *66*, 93–101. doi:10.1016/j.dss.2014.06.008

ENISA. (2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. Retrieved from ENISA website: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

Faily, S. (2018). Introducing CAIRIS: Tool-support for designing usable and secure systems. In *Designing Usable and Secure Software with IRIS and CAIRIS* (pp. 89–118). doi:10.1007/978-3-319-75493-2_5

Felstead, A., & Henseke, G. (2017). Assessing the growth of remote working and its consequences for effort, well-being and work-life balance. *New Technology, Work and Employment*, *32*(3). doi:10.1111/ntwe.12097

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80–92. doi:10.1177/160940690600500107

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs - Principles and practices. *Health Services Research*, *48*(6 PART2). doi:10.1111/1475-6773.12117

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183. doi:10.1016/j.cose.2016.06.002

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988. doi:10.1016/j.cose.2012.08.004

Furnell, S., & Shah, J. N. (2020). Home working and cyber security – an outbreak of unpreparedness? *Computer Fraud and Security*, *2020*(8). doi:10.1016/S1361-3723(20)30084-1

Gable, G. G., & Gable, G. G. (2016). Integrating case study and survey research methods: An example in information systems. In *Case Studies* (pp. 211–211). doi:10.4135/9781473915480.n12

Gangire, Y., Da Veiga, A., & Herselman, M. (2020). Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory. *Human Aspects of Information Security and Assurance*, 144–157. doi:10.1007/978-3-030-57404-8_12

Godlove, T. (2012). Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines. *Information Security Journal: A Global Perspective*, *21*(4), 216–229. doi:10.1080/19393555.2012.668747

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People*, *39*, 88. doi:10.1108/09593840910962186

Guest, G., MacQueen, K. M., & Namey, E. E. (2011). *Applied Thematic Analysis*. Retrieved from https://play.google.com/store/books/details?id=Hr11DwAAQBAJ

Guetterman, T. C., Fetters, M. D., & Creswell, J. W. (2015). Integrating quantitative and qualitative results in health science mixed methods research through joint displays. *Annals of Family Medicine*, *13*(6). doi:10.1370/afm.1865

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers and Security*, Vol. 32. doi:10.1016/j.cose.2012.10.003

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2). doi:10.2753/MIS0742-1222280208

Haeussinger, F., & Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. *ICIS 2013 Proceedings*. Retrieved from https://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/9/

Hanson, W. E., Plano Clark, V. L., Petska, K. S., Creswell, J. W., & Creswell, J. D. (2005). Mixed methods research designs in counseling psychology. *Journal of Counseling Psychology*, Vol. 52. doi:10.1037/0022-0167.52.2.224

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2). doi:10.1016/j.dss.2009.02.005

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*. doi:10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1). doi:10.1016/j.im.2013.10.001

Ifinedo, P. (2019). Investigating employee engagement in nonmalicious, end-user computing and information security deviant behavior. *25th Americas Conference on Information Systems, AMCIS 2019*.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. doi:10.1016/j.jcss.2014.02.005

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75–87. doi:10.1016/j.chb.2016.09.012

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). 'Shadow security' as a tool for the learning organization. *ACM SIGCAS Computers and Society*, *45*(1). doi:10.1145/2738210.2738216

Kirlappos, Parkin, S., & Sasse, M. A. (2014). *Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security*. doi:10.14722/usec.2014.23007

Koskey, K. L. K., & Stewart, V. C. (2014). A Concurrent Mixed Methods Approach to Examining the Quantitative and Qualitative Meaningfulness of Absolute Magnitude Estimation Scales in Survey Research. *Journal of Mixed Methods Research*, *8*(2), 180–202. doi:10.1177/1558689813496905

Kroll, T., & Neri, M. (2009). Designs for Mixed Methods Research. In *Mixed Methods Research for Nursing and the Health Sciences*. doi:10.1002/9781444316490.ch3

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685–692. doi:10.1016/s0167-4048(03)00007-5

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707–718. doi:10.1016/j.im.2003.08.008

Leech, N. L., & Onwuegbuzie, A. J. (2009). A typology of mixed methods research designs. *Quality and Quantity*, *43*(2). doi:10.1007/s11135-007-9105-3

Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions - Planned behavior, reasoned action, perceived importance, or individual characteristics? *Information and Management*, *42*(1). doi:10.1016/j.im.2003.12.008

Lietz, P. (2010). Research into questionnaire design: A summary of the literature. *International Journal of Market Research*, *52*(2), 249–272. doi:10.2501/s147078530920120x

Lincoln, Y. S., Lynham, S. A., Guba, E. G., & Others. (2011). Paradigmatic controversies, contradictions, and emerging confluences, revisited. *The Sage Handbook of Qualitative Research*, *4*, 97–128. Retrieved from https://books.google.co.za/books?hl=en&lr=&id=qEiC-_ELYgIC&oi=fnd&pg=PA97&ots=C4iVzkKr1G&sig=E_v2IRfo4xaYbgQSdLsjZxt63Z8

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly: Management Information Systems*, *16*(2). doi:10.2307/249574

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. doi:10.1016/j.chb.2016.11.065

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative Research: A Guide to Design and Implementation*. Retrieved from https://play.google.com/store/books/details?id=JFN_BwAAQBAJ

Morris, E., & Burkett, K. (2011). Mixed methodologies: A new research paradigm or enhanced quantitative paradigm. *Online Journal of Cultural Competence in Nursing and Healthcare*, *1*(1), 27–36. doi:10.9730/ojccnh.org/v1n1a3

Ng, B. Y., & Rahim, M. A. (2005). A socio-behavioral study of home computer users' intention to practice security. *9th Pacific Asia Conference on Information Systems: I.T. and Value Creation, PACIS 2005*.

Ng, B.-Y., & Rahim, M. (2005). *A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security*. Retrieved from https://www.semanticscholar.org/paper/4f97a6e017a4a1c6d7ba7440056785b9ee3faab2

Noonan, M., & Glass, J. (2012, December 4). Telecommuting increases work hours and blurs boundary between work and home, new study shows.

Science Daily. Retrieved from https://www.sciencedaily.com/releases/2012/12/121204145826.htm

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1), 1609406917733847. doi:10.1177/1609406917733847

Okereafor, K., & Manny, P. (2020). *UNDERSTANDING CYBERSECURITY CHALLENGES OF TELECOMMUTING AND VIDEO CONFERENCING APPLICATIONS IN THE COVID-19 PANDEMIC* (Vol. 8).

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *SSRN Electronic Journal*. doi:10.2139/ssrn.1954824

Oltsik, J. (2020). ESG Research Report: The Impact of the COVID-19 Pandemic on Cybersecurity. Retrieved 1 July 2021, from https://www.esg-global.com/research/esg-research-report-the-impact-of-the-covid-19-pandemic-on-cybersecurity

Onwuegbuzie, A., Leech, N., & Collins, K. (2015). Qualitative analysis techniques for the review of the literature. *The Qualitative Report*. doi:10.46743/2160-3715/2012.1754

Onwuegbuzie, & Collins. (2007). A typology of mixed methods sampling designs in social science research. *The Qualitative Report*, *12*(2).

Pardede, P. (2019). Mixed Methods Research Designs in EFL 1. *Proceeding of EED Collegiate Forum 2015-2018* │, (April 2018).

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

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

Pattinson, M. R., Butavicius, M. A., Parsons, K., McCormac, A., & Jerram, C. (2015). Examining Attitudes toward Information Security Behaviour using Mixed Methods. *HAISA*, 57–70. Retrieved from https://books.google.com/books?hl=en&lr=&id=NQJqCwAAQBAJ&oi=fnd&pg=PA57&dq=Examining+attitudes+toward+information+security+behaviour+usingmixed+methods&ots=bpENARG4oJ&sig=bXrFjjDDz-V2tPqfQUmW4NFbrbw

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4). doi:10.1515/jhsem-2014-0035

Popescu, G. (2014). Human Behavior, from Psychology to a Transdisciplinary Insight. *Procedia - Social and Behavioral Sciences*, *128*, 442–446. doi:10.1016/j.sbspro.2014.03.185

PwC. (2020). *When the boardroom becomes the battlefield*. Retrieved from https://www.pwc.co.za/en/assets/pdf/global-economic-crime-survey-2020.pdf

Rader, E., & Wash, R. (2015). Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, *1*(1), 121–144. doi:10.1093/cybsec/tyv008

Reddy, N., & Reddy, U. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Retrieved from http://arxiv.org/abs/1402.1842

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

Rupietta, K., & Beckmann, M. (2018). Working from Home. *Schmalenbach Business Review*, *70*(1), 25–55. doi:10.1007/s41464-017-0043-x

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. doi:10.1016/j.cose.2015.05.012

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*. Retrieved from https://link.springer.com/article/10.1023/A:1011902718709

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *International Journal of Electronic Security and Digital Forensics*. Retrieved from https://repository.uel.ac.uk/item/84v3v

Schneier, B. (Ed.). (2003). Systems and How They Fail. In *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (pp. 47–58). doi:10.1007/0-387-21712-6_4

Shillair, R. (2016). Instilling a security mindset: Getting into the cat and mouse game. *SSRN Electronic Journal*. doi:10.2139/ssrn.2756736

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. doi:10.1016/j.cose.2015.01.002

Simonet, J., & Teufel, S. (2019). The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users. *ICT Systems Security and Privacy Protection*, 194–208. doi:10.1007/978-3-030-22312-0_14

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. doi:10.1016/j.im.2013.08.006

Smith, R. (2012). A contemporary look at Saltzer and Schroeder's 1975 design principles. *IEEE Security & Privacy*, 1–1. doi:10.1109/msp.2012.85

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. doi:10.1016/j.cose.2015.10.006

Souppaya, M., & Scarfone, K. (2016). *NIST Special Publication 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security*. doi:10.6028/NIST.SP.800-114r1

Spitzmüller, C., & Stanton, J. M. (2006). Examining employee compliance with organizational surveillance and monitoring. *Journal of Occupational and Organizational Psychology*, *79*(2), 245–272. doi:10.1348/096317905x52607

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2). doi:10.1016/j.cose.2004.07.001

Stephanou, A. T., & Dagada, R. (2014). The Impact of Information Security Awareness Training on Information Security Behaviour: the Case for further Research. *Information Security and Cryptography*.

Straub, D. W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *The Mississippi Quarterly*, *14*(1). doi:10.2307/249307

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*. doi:10.1109/ARES.2010.27

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, *23*(2), 1–11. Retrieved from https://smartlib.umri.ac.id/assets/uploads/files/24c10-impact-of-cyberattacks-on-financial-institutions.pdf

Tashakkori, A., & Creswell, J. W. (2007). Editorial: Exploring the Nature of Research Questions in Mixed Methods Research. *Journal of Mixed Methods Research*, *1*(3), 207–211. doi:10.1177/1558689807302814

Tashakkori, A., & Teddlie, C. (2010). SAGE Handbook of Mixed Methods in Social and Behavioral Research. In *Second edition. Los Angeles and London: Sage Publications, 2010, pp. xv, 893*.

Tashakkori, A., Teddlie, C., Plano Clark, V., & Badiee, M. (2015). Research Questions in Mixed Methods Research. In *SAGE Handbook of Mixed Methods in Social & Behavioral Research*. doi:10.4135/9781506335193.n12

Teddlie, C., & Yu, F. (2007). Mixed methods sampling. *Journal of Mixed Methods Research*, *1*(1), 77–100. doi:10.1177/2345678906292430

Terekhova, M. (2018, March 8). Financial and economic heavy hitters have formed a cybersecurity consortium. Retrieved 2 March 2021, from Business Insider website: https://www.businessinsider.com/financial-economic-heavy-hitters-cybersecurity-consortium-2018-3?IR=T

The International Telecommunication Union. (2009). *Overview of cybersecurity*. Retrieved from The International Telecommunication Union website: https://www.itu.int/rec/T-REC-X.1205-200804-I

The National Institute of Standards and Technology. (2020). Cybersecurity. Retrieved 28 January 2021, from https://csrc.nist.gov/glossary/term/cybersecurity

van Rensburg, R. J. (2020, July 2). South Africa's POPI Act. Retrieved 17 March 2021, from Solidarite IT website: https://www.privacypolicies.com/blog/popi-act/

Venkatesh, V., University of Arkansas, Brown, S., Sullivan, Y., University of Arizona, & State University of New York, Binghamton. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, *17*(7), 435–494. doi:10.17705/1jais.00433

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security--what goes where? *Information & Computer Security*. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2017-0025/full/html

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*. doi:10.1016/j.cose.2013.04.004

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101–105. doi:10.1057/ejis.2009.12

Whitten, A., & Tygar, J. D. (1999, August 23). Why Johnny can't encrypt: a usability evaluation of PGP 5.0. *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, 14. Presented at the Washington, D.C. Retrieved from https://dl.acm.org/doi/10.5555/1251421.1251435

Wong, W. P., Tan, H. C., Tan, K. H., & Tseng, M.-L. (2019). Human factors in information leakage: mitigation strategies for information sharing

integrity. *Industrial Management + Data Systems*, *119*(6), 1242–1267. doi:10.1108/imds-12-2018-0546

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6). doi:10.1016/j.chb.2008.04.005

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology* , *58*(2). doi:10.1002/asi.20474

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace. *Information Technology & People*, *26*(4), 401–419. doi:10.1108/itp-12-2012-0147

Zakaria, O. (2006). Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge. *Security and Privacy in Dynamic Environments*, 437–441. doi:10.1007/0-387-33406-8_38

Zheng, Z., Cheng, H., Zhang, Z., Zhao, Y., & Wang, P. (2018). An alternative method for understanding user-chosen passwords. *Security and Communication Networks*, *2018*, 1–12. doi:10.1155/2018/6160125

APPENDIX A: Interview Request

Dear Sir/Madam

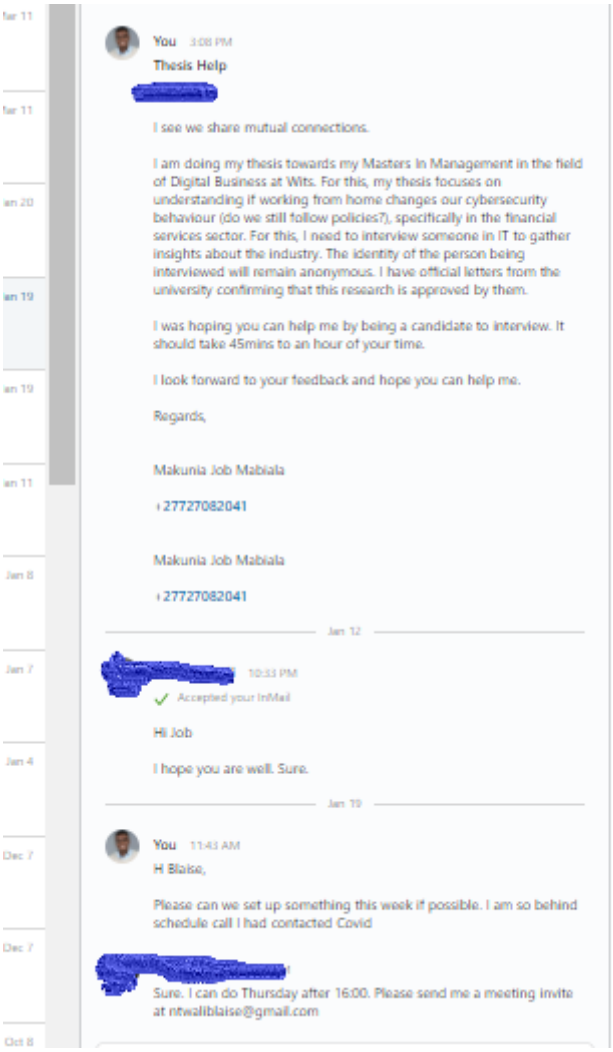
My name is Makunia Job Mabiala, a Masters student In Digital Business at University of Witwatersrand in South Africa. I invite you to participate in an academic study of 'The role of remote working on Cybersecurity behaviour of South African Financial Services employees'.

The aim of this study is to understand the role remote working on cybersecurity behaviour. Remote working has grown in popularity and will be the new way of working. The research will uncover the experience with employees working remotely and understand how it influences their cybersecurity behaviours. Understanding behaviours that usually take place within company parameters and whether this is retained when employees work remotely will enable the researcher to present factors that influence the behaviours.

Qualitative data for this research will be obtained from video aided interviews. Participation in this research is entirely voluntary and I anticipate that your engagement will require approximately 60 minutes of your time. Withdrawal from the research is possible at any time prior to the data I am collecting being analysed. You can stop the interview at any time. In any event, your contribution to my research will be in confidence and references in my final published research will be anonymous. It should also be noticed that the data belongs to the researcher and the University of Witwatersrand. And the data cannot be used for human resources or employment progression issues. If your permission is obtained and no withdrawal is requested, the researcher will include material from the interview for the researcher's Masters Thesis and, possibly, other relevant publications.

If you have a concern on any aspect of this interview or study, you may contact me via e-mail 2400426@students.wits.ac.za or by telephone on +27727082041. If there are any ethical concerns, you can also contact my advisor, Dr Kiru Pillay (kiru2010@gmail.com).

If you have any further questions, please feel free to contact me. Thank you for sharing your time for this interview. Your participation is greatly appreciated.



You 3:08 PM

Thesis Help

[redacted]

I see we share mutual connections.

I am doing my thesis towards my Masters in Management in the field of Digital Business at Wits. For this, my thesis focuses on understanding if working from home changes our cybersecurity behaviour (do we still follow policies?), specifically in the financial services sector. For this, I need to interview someone in IT to gather insights about the industry. The identity of the person being interviewed will remain anonymous. I have official letters from the university confirming that this research is approved by them.

I was hoping you can help me by being a candidate to interview. It should take 45mins to an hour of your time.

I look forward to your feedback and hope you can help me.

Regards,

Makunia Job Mabiala

+27727082041

Makunia Job Mabiala

+27727082041

Jan 12

[redacted] 10:33 PM

Accepted your InMail

Hi Job

I hope you are well. Sure.

Jan 19

You 11:43 AM

H Blaise,

Please can we set up something this week if possible. I am so behind schedule call I had contacted Covid

[redacted]

Sure. I can do Thursday after 16:00. Please send me a meeting invite at ntwaliblaise@gmail.com

APPENDIX B: Interview Protocol

Semi-structured Interview Instrument: Qualitative method

1. How would you describe your overall company security culture/approach to cybersecurity?

Probe (Theory of Planned Behaviour):

   a. What attitudes do employees generally have toward cybersecurity? This refers to an employee's disposition (i.e. inclination or tendency) to respond favourably or unfavourably towards practising computer security.
   b. Is cybersecurity mainly seen as an IT problem?
   c. Would employees call each other out if they were violating cybersecurity rules?
   d. Do they understand the threats and risks associated with cybersecurity breaches?

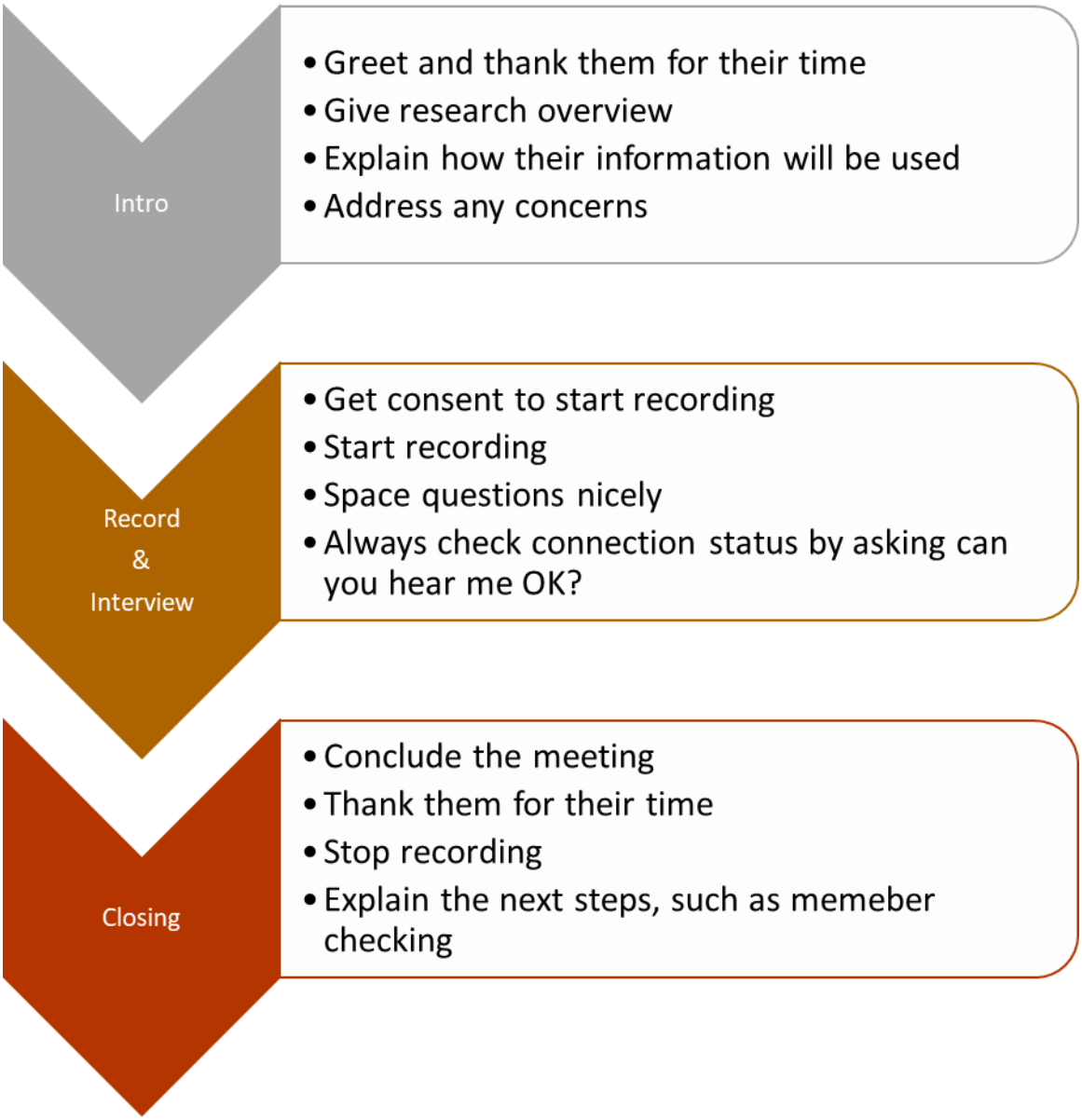
2. Tell me about the cybersecurity training you provide to employees

   a. What type of training do you put in place?
   b. What do they cover? **(behaviours)**
   c. How frequently do these occur?
   d. How easy is it for employees to access?
   e. How do you assess or measure the level of compliance?

3. How do you ensure that employees behave safely in the office environment?

   a. Do you have dedicated policies and procedures?
   b. How is accessible are the policies and procedures?
   c. What are critical do's and don't when employees work remotely (should inform behaviours)
   d. How do you monitor policy violations?
   e. What is your company's stance on BYOD and mobile devices?

Interview strategy



APPENDIX C: Summary of thematic analysis

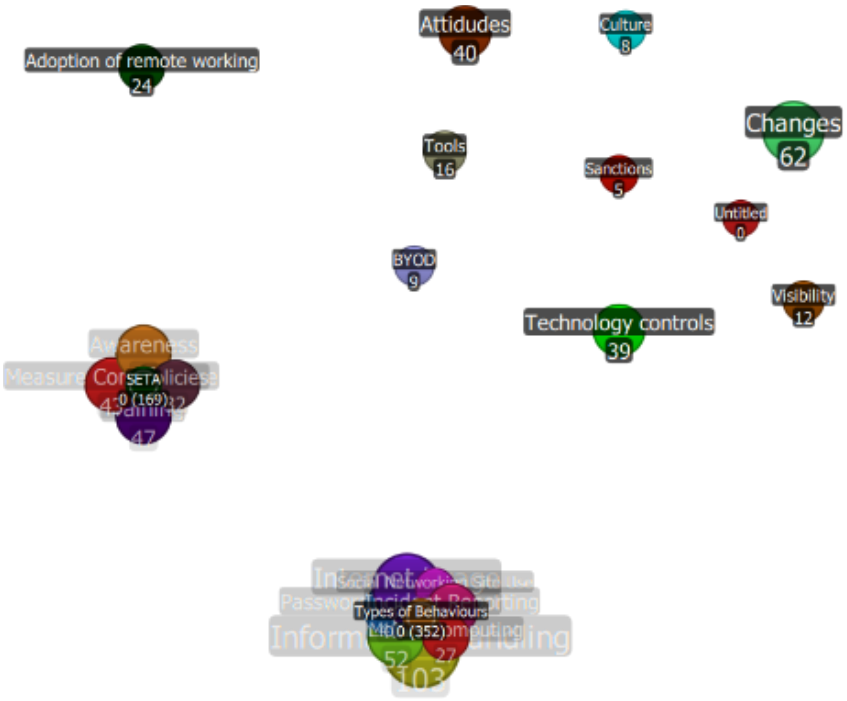
Quirkos

Quirkos Report

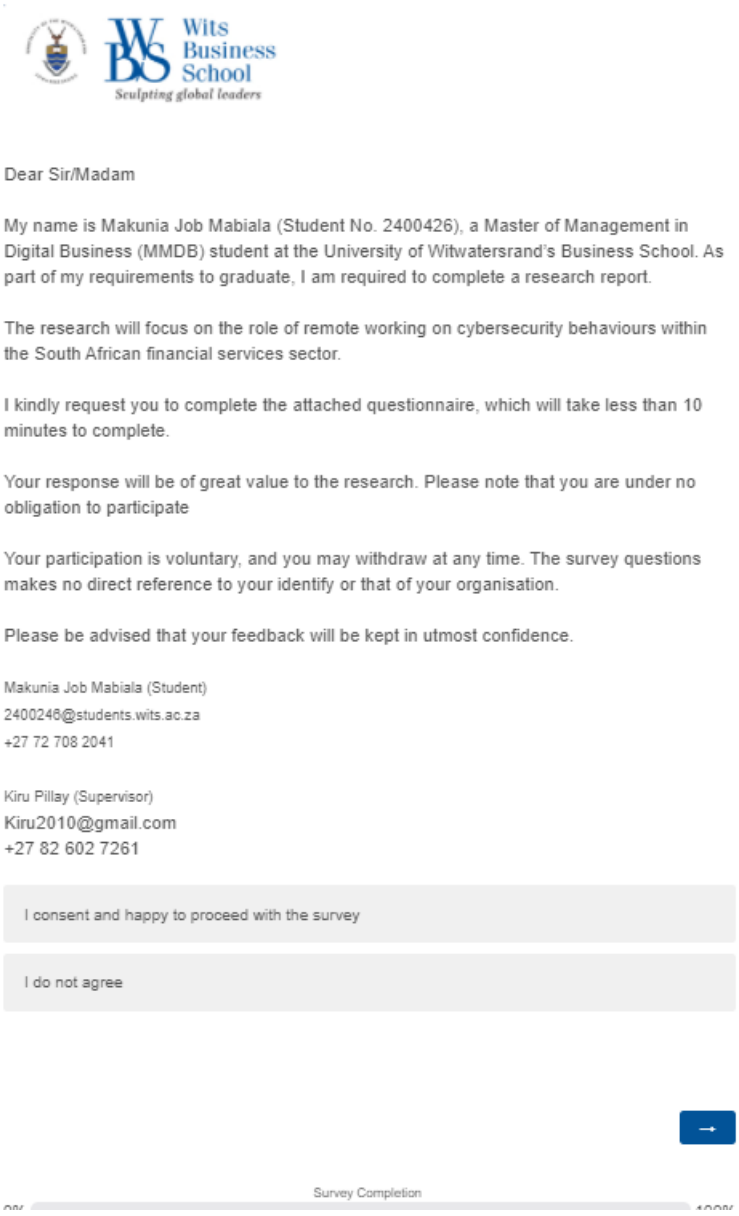
Source Summary

Title	Author	Length	Quotes #
Participant A	Job Mabiala	11220	38
Participant PS	Job Mabiala	25986	75
Participant NM	Job Mabiala	21725	28
Participant KM	Job Mabiala	54864	128
Participant SL	Job Mabiala	42739	171
Participant B	Job Mabiala	29971	128
Partcipant D	Job Mabiala	39528	110
Participant T	Job Mabiala	24149	58

Quirks Canvas - Primary



APPENDIX D: Instrument – Questionnaire



Wits Business School
Sculpting global leaders

Dear Sir/Madam

My name is Makunia Job Mabiala (Student No. 2400426), a Master of Management in Digital Business (MMDB) student at the University of Witwatersrand's Business School. As part of my requirements to graduate, I am required to complete a research report.

The research will focus on the role of remote working on cybersecurity behaviours within the South African financial services sector.

I kindly request you to complete the attached questionnaire, which will take less than 10 minutes to complete.

Your response will be of great value to the research. Please note that you are under no obligation to participate

Your participation is voluntary, and you may withdraw at any time. The survey questions makes no direct reference to your identify or that of your organisation.

Please be advised that your feedback will be kept in utmost confidence.

Makunia Job Mabiala (Student)
2400246@students.wits.ac.za
+27 72 708 2041

Kiru Pillay (Supervisor)
Kiru2010@gmail.com
+27 82 602 7261

I consent and happy to proceed with the survey

I do not agree

→

Survey Completion



Please indicate to what extent you agree or disagree with each of the statements below

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
My family members/friends positively influence my safe cybersecurity behaviour when I work remotely (they call me out if they notice I am not being safe such as leaving my screen unlocked and unattended)	O	O	O	O	O
My family members/friends would expect me to practice safe cyber behaviours when I work remotely	O	O	O	O	O
Hearing news about cybersecurity incidents encourages me to practice safe cybersecurity behaviours when I work remotely	O	O	O	O	O
It seems that all mass media encourages safe cybersecurity behaviour when working remotely	O	O	O	O	O
I feel under pressure from the mass media to practice safe cybersecurity behaviour when working remotely	O	O	O	O	O

←

→

Survey Completion

0% 100%

Wits Business School
Sculpting global leaders

Please indicate to what extent you agree or disagree with each of the statements below

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
I feel aware of cyberseourity risks and threats that come with working remotely	O	O	O	O	O
I feel that it is my responsibility to protect myself from cyberseourity risks and threats when working remotely	O	O	O	O	O
I feel that issues stemming from cyberseourity risks and threats are not of significance when working remotely	O	O	O	O	O
I feel that there's no need to protect myself when working remotely because I will not be exposed to cyberseourity risks and threats	O	O	O	O	O
I follow cyberseourity rules only if it does not interfere with my productivity	O	O	O	O	O
I am aware of cyberseourity policies but do not have the time to follow them when working remotely	O	O	O	O	O
I do not understand why I should use seourity measures when I work remotely	O	O	O	O	O
I believe that I am at risk of becoming a victim of a cyberseourity incident (e.g. phishing, malware)	O	O	O	O	O
I believe that it is likely that I will become a victim of a cyberseourity incident (e.g. phishing, malware)	O	O	O	O	O

← →

Survey Completion
0% 100%



Please indicate to what extent you agree or disagree with each of the statements below

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
My organization's cybersecurity policies on remote working are written in a manner that is clear and understandable	○	○	○	○	○
My organization's cybersecurity policies are readily available for my reference	○	○	○	○	○
My organization provides training to help employees improve their assessment and knowledge of computer and cybersecurity issues when working remotely	○	○	○	○	○
My organization disciplines employees who violate cybersecurity policies	○	○	○	○	○

← →

Survey Completion

0% 100%



Please indicate to what extent you agree or disagree with each of the statements below

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
When working remotely, I will continue to comply with cybersecurity policies that I usually follow when working in the office	○	○	○	○	○
Complying with cybersecurity policies is entirely under my control	○	○	○	○	○
Complying with my organization's cybersecurity policies is easy	○	○	○	○	○

←

→

Survey Completion

0% 100%

APPENDIX E: Financial Services LinkedIn Group

