

https://dspace.org/

The impact of work from home and hybrid mode on cybersecurity practices in South Africa

Pather, Ravashalin

2023
University of the Witswatersrand, Johannesburg
https://hdl.handle.net/10539/38535

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

The impact of work from home and hybrid mode on cybersecurity practices in South Africa.

Ravashalin Pather

1806289

1806289@students.wits.ac.za

+27829988584

A research proposal 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, 2023

DECLARATION

I, Ravashalin Pather, declare that this study entitled *"The impact of work from home and hybrid mode on cybersecurity practices in South Africa".* has been composed solely by myself. I have acknowledged, credited, and referenced all sources and information. I also declare that this research paper has not been submitted, in any previous application for a degree. I am hereby submitting it in fulfilment of the requirements of the degree of Master of Management: in the field of Digital Business at the University of the Witwatersrand, Johannesburg.



Ravashalin Pather

Signed at Johannesburg on 16th June 2023

Name of candidate	**Ravashalin Pather**
Student number	**1806289**
Telephone numbers	**+27 82 998 8584**
Email address	**1806289@students.wits.ac.za**
First year of registration	**2022**
Date of proposal submission	**25-08-2022**
Date of Ethics Clearance	**20-12-2022**
Date of report submission	**27-06-2023**
Name of supervisor	**Dr Kiru Pillay**

ABSTRACT

As the trend of work-from-home and remote work grows in South Africa, adopting adequate cybersecurity measures and evaluating the human aspect of security perceptions is critical in protecting organisational information and maintaining corporate integrity. Over the past two decades, cybersecurity has been viewed from technological perspective of protecting networks and information assets, this study invokes the behavioural and social concerns, and how this affects an organisation's cybersecurity strategy in South Africa. Covid-19 and the lockdown rules triggered a national emergency, compelling a considerable proportion of South Africa's workforce to embrace a work-from-home culture. While this study began during the lockdown, leaders at large enterprises in South Africa are adopting a more hybrid way of working permanently, due to the subsequent benefits. This study aimed to evaluate employee behaviour when working environments are suddenly affected by work-from-home policies and how an employee's behaviour transposes to a different location. The overarching question was: How has cybersecurity behaviour in South Africa manifested during work-from-home policies and what are the determinants that force correct cybersecurity compliant behaviour?. Four key factors *("Subjective Norms & Response Efficacy", "Attitude & Perceived Vulnerability", "Self-Efficacy" and "Perceived Severity")* were identified and combined into a new framework based of two theoretical frameworks (The Theory of Planned Behaviour and Protection Motivation theory). This study utilised a quantitative cross-sectional design using a structured closed questionnaire that was distributed electronically. The data collected from 186 participants were analysed using Exploratory factor analysis, correlation analysis and multiple regression. Overall, *"Subjective Norms & Response Efficacy"* emerged as a significant and most influential predicator of *"Cybersecurity Compliant behaviour*". "*Attitude & Perceived Vulnerability*", "*Self-Efficacy*" and "*Perceived Severity*" were insignificant. It is apparent that there is a positive perception of correct Cyber security practices amongst South African organisations however there is a recommendation for future research, due to the diversity of organisational leadership in both the private and state-owned entities, to provide a better understanding of security compliant behaviour.

KEYWORDS

Cybersecurity, COVID-19, Protection Motivation Theory, Theory of Planned Behaviour. Work-from-home, Remote work, Lockdown, Cyber Security Behaviour.

TABLE OF CONTENTS

DECLARATION ii
ABSTRACT…. iii
KEYWORDS…. iv
TABLE OF CONTENTS v
LIST OF TABLES ix
LIST OF FIGURES xii
ACKNOWLEDGEMENTS xiii
LIST OF ACRONYMS xiv
1. INTRODUCTION TO THE RESEARCH 15
1.1 Statement of purpose 15
1.2 Background of the study 15
1.2.1 Lasting Cyber Risks introduced by the Pandemic lockdown. 16
1.2.2. Increased Security Risk from Remote Working 17
1.2.3. Post COVID-19 Posture 18
1.3. Research problem 18
1.4. Research objectives 19
1.5. Rationale 20
1.6. Delimitations 21
1.7. Definition of terms 21
1.8. Assumptions 22
1.9. Chapter Outline 22
2. LITERATURE REVIEW 24
2.1. The Human Aspect of Cybersecurity 24
2.1.1. Work from Home/Hybrid working. 25
2.1.2. Cybersecurity Compliant Behaviour 25
2.2. Definition of Key Constructs 26
2.2.1. Employee Threat Assessment 26
2.2.1.1. Threat severity 27
2.2.1.2. Perceived vulnerability 27
2.2.2. Employee efficacy 28
2.2.2.1. Response Efficacy 29
2.2.2.2. Self-efficacy 29
2.2.3. Attitude 30
2.2.4. Subjective Norms 31
2.3. Analytical Framework 31
2.3.1. Theoretical Frameworks of Cybersecurity Compliance 32

2.3.2. Conceptual Framework 34
2.4. Conclusion of Literature Review 35
3. RESEARCH METHODOLOGY 37
3.1. Research Philosophy 37
3.2. Research approach 37
3.3. Research design 38
3.4. Data Collection and the Research Instrument. 39
3.5. Population and sample 40
3.5.1. Population 40
3.5.2. Sampling method 41
3.5.3. Sample 41
3.5.4. Sample size 42
3.6. Data analysis strategies and interpretation 42
3.6.1. Statistical Assumptions 42
3.6.1.1. Outliers 43
3.6.1.2. Multicollinearity 43
3.6.1.3. Linearity 44
3.7. Quality Assurance 44
3.7.1. Reliability 44
3.7.2. Validity 45
3.8. Statistical Techniques 46
3.8.1. Exploratory Factor Analysis (EFA) 46
3.8.1.1. Inter Item Correlation 47
3.8.1.2. Extraction of Factors. 47
3.8.1.3. Factor Rotation 47
3.8.2. Multiple Regression Analysis 48
3.9. Ethical considerations 48
4. PRESENTATION OF RESEARCH RESULTS 50
4.1. Description of Research respondents 50
4.1.1. Work from home 50
4.2. Descriptive Statistics Analysis 52
4.3. Self-Efficacy 54
4.3.1. Presentation of the Empirical Results 54
4.4. Attitude towards Cyber Security 55
4.4.1. Presentation of the Empirical Results 55
4.5. Perceived Vulnerability 56
4.5.1. Presentation of the Empirical Results 56

4.6. Perceived Severity 57
4.6.1. Presentation of the Empirical Results 57
4.7. Subjective Norms 58
4.7.1. Presentation of the Empirical Results 58
4.8. Response efficacy towards Cyber Security 59
4.8.1. Presentation of the Empirical Results 59
4.9. Dependant Variable: Cybersecurity compliant behaviour 59
4.9.1. Presentation of the Empirical Results 60
4.10. Exploratory Factor Analysis 60
4.10.1. Cybersecurity Compliant Behaviour (Dependant Variable) 61
4.10.1.1. Factor Extraction 62
4.10.2. Independent Variables 63
4.10.2.1. Factor Extraction 63
4.10.3. 2nd Order Factor Analysis 65
4.11. Theoretical, Empirical Reliabilities and Correlations 67
4.11.1. Self-Efficacy 67
4.11.2. Attitude 68
4.11.3. Perceived Vulnerability 69
4.11.4. Perceived Severity 69
4.11.5. Subjective Norms 70
4.11.6. Response Efficacy 71
4.11.7. Cyber security compliant behaviour (Dependent Variable) 72
4.11.8. Subjective Norms & Response Efficacy (Empirical) 72
4.11.9. Attitude & Perceived Vulnerability (Empirical) 73
4.12. Summary of Reliability 73
4.13. Updated Model and Hypothesis 74
4.14. Descriptives on Scales 76
4.15. Statistical Hypothesis Testing Between Variables 76
4.15.1. Statistical assumptions 76
4.15.1.1. Outliers 76
4.15.1.2. Multicollinearity 77
4.15.1.3. Sample Size 78
4.15.1.4 Linearity 78
4.15.2. Correlation Results 78
4.15.3. Overall fit of the model 79
4.15.2.1 Model Summary 79
4.15.2.2. ANOVA results 80

4.15.4. Multiple Linear Regression 80
4.15.5. H1 – Influence of Subjective Norms & Response Efficacy to Cybersecurity Compliant Behaviour 81
4.15.6. H2 - Influence of Attitude & Perceived Vulnerability to Cybersecurity Compliant Behaviour 82
4.15.7. H3 - Influence of Self-Efficacy to Cybersecurity Compliant Behaviour 82
4.15.8. H4 - Influence of Perceived Severity to Cybersecurity Compliant Behaviour 83
4.16. Chapter Summary 83
5. DISCUSSION OF RESEARCH FINDINGS 85
5.1. Brief Contextual Background 85
5.2. Influence of Subjective Norms & Response Efficacy toward Cybersecurity Compliant Behaviour. 86
5.3. Influence of Attitude and Perceived Vulnerability toward Cybersecurity Compliant Behaviour. 88
5.4. Influence of Self-efficacy toward Cybersecurity Compliant Behaviour. 89
5.5. Influence of Perceived severity toward Cybersecurity Compliant Behaviour. 89
5.6. Summary and Conclusion of Research Findings 90
6. RECOMMENDATIONS AND LIMITATIONS 92
6.1. Recommendations For Organisations 92
6.2. Recommendations For Researchers 92
6.3. Limitations 93
6.4. Conclusion 94
REFERENCES 95
APPENDIX A: DATA COLLECTION INSTRUMENT 102
Cover Letter for Research Instrument 102
Research instrument 103
Consistency Matrix 112
Ethic Clearance Document 113
APPENDIX B: EXPLORATORY FACTOR ANALYSIS 114
APPENDIX C: REGRESSION MODEL 117

LIST OF TABLES

Table 1: Summary of Items per Construct 40

Table 2: Cronbach Alpha on Theoretical constructs 45

Table 3: Frequencies of Measures for Demographic 52

Table 4: Key Factors that Influence Cybersecurity behaviour. 53

Table 5: Descriptive Statistics - Self-efficacy 55

Table 6: Descriptive Statistics - Attitude towards Cybersecurity 56

Table 7: Descriptive Statistics - Perceived Vulnerability 57

Table 8: Descriptive Statistics - Perceived Severity 58

Table 9: Descriptive Statistics - Subjective norms 58

Table 10: Descriptive Statistics - Response Efficacy 59

Table 11: Descriptive Statistics - Cybersecurity Compliant behaviour 60

Table 12: Inter Item Correlation Coefficients (Cybersecurity Compliant Behaviour) 61

Table 13: KMO and Bartlett's Test (Cybersecurity Compliant Behaviour). 62

Table 14: Total Variance Explained (Cybersecurity Compliant Behaviour). 62

Table 15: KMO and Bartlett's Test 63

Table 16: Total Variance Explained. 64

Table 17: Rotated Factor Matrix. 65

Table 18: Correlation Matrix (Independent Factors) 66

Table 19: KMO and Bartlett's Test (2nd order Factor Analysis). 66

Table 20: Total Variance Explained (2nd Order Factor Analysis). 66

Table 21: Item-Total Statistics (Self-Efficacy) 67

Table 22: Inter Item Correlation (Self-Efficacy) 68

Table 23: Item-Total Statistics (Attitude) 68

Table 24: Inter Item Correlation (Attitude) 68

Table 25: Item-Total Statistics (Perceived Vulnerability) 69

Table 26: Inter Item Correlation (Perceived Vulnerability) 69

Table 27: Item-Total Statistics (Perceived Severity) 70

Table 28: Inter Item Correlation (Perceived Severity) 70

Table 29: Item-Total Statistics (Subjective Norms) 70

Table 30: Inter Item Correlation (Subjective Norms) 71

Table 31: Item-Total Statistics (Response-Efficacy) 71

Table 32: Inter Item Correlation (Response Efficacy) 71

Table 33: Item-Total Statistics (Cyber security compliant behaviour) 72

Table 34: Subjective Norms & Response Efficacy (Empirical) 72

Table 35: Attitude & Perceived Vulnerability (Empirical) 73

Table 36: Cronbach Alpha for Internal Reliability (Theoretical) 74

Table 37: Cronbach Alpha for Internal Reliability (Empirical) 74

Table 38: Scale Descriptives 76

Table 39: Residual Statistics (Outliers Removed) 77

Table 40: Collinearity Coefficients 77

Table 41: Pearson Correlation for All Constructs 79

Table 42: Model Summary 80

Table 43: ANOVA results 80

Table 44: Multiple Regression Model Summary 81

Table 45: Hypothesis Summary Table 84

Table 46 : Consistency Matrix 112

Table 47: Communalities for Cybersecurity Compliant Behaviour 114

Table 48: Anti image (Cybersecurity Compliant behaviour) 114

Table 49: Factor Matrix for Cybersecurity Compliant Behaviour 114

Table 50: Communalities for Independent Variables 114

Table 51: Anti-image Matrices (Independent Variables) 115

Table 52: Communalities for 2nd Order Factor Analysis 115

Table 53: Factor Matrix for 2nd Order Factor Analysis 115

Table 54: Anti-image Matrices (Cybersecurity Compliant Behavior) 116

Table 55: Collinearity Diagnostics 116

Table 56: Residual Statistics (Outliers present) 117

LIST OF FIGURES

Figure 1: The Protection Motivation Theory Model.....33

Figure 2: The Theory of Planned Behaviour Model.....34

Figure 3: Research Model - Adapted from the Protection Motivation Theory and the Theory of Planned Behaviour.....35

Figure 4: Work from Home.....51

Figure 5: Sample Distribution.....51

Figure 6: New Model for Regression Analysis.....75

Figure 7: Histogram of Regression Standardise Residuals with Outliers.....117

Figure 8: Histogram of Regression Standardise Residuals - Outliers Removed.....117

Figure 9: Scatterplot.....117

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Mr Kiru Pillay for the support, knowledge, and prompt feedback throughout this endeavour, allowing us to engage at any part of the day or night.

To my wife Tanya, my daughters Tiara and Gianna, I thank you for allowing me time and space to complete this research paper. It was a long, personal journey for me; however, your encouragement and support are truly appreciated.

And finally, to my mother, for her sacrifices and guidance throughout my childhood. I sincerely thank you; your support has shaped me into the person I am today. My endurance and ability to pursue my academic goals can only be attributed to your vision for my future, 45 years ago.

LIST OF ACRONYMS

Covid-19	Coronavirus
ICT	Information and Communications Technology
IT	Information Technology
KMO	Kaiser-Meyer-Olkin
MFA	Multi-Factor Authentication
PBC	Perceived Behavioural Control
PMT	Protection Motivation Theory
RSA	Republic of South Africa
SN	Subjective Norm
SPSS	Statistical Package for Social Sciences
TPB	Theory of Planned Behaviour
VPN	Virtual Private Networks
WFH	Work from home
WHO	World Health Organisation

1. INTRODUCTION TO THE RESEARCH

The terminology and concepts used to conceptualize this research study are briefly introduced in Chapter 1. Section 1.1 covers the statement of purpose, followed by the background of the study on section 1.2. Thereafter the research problem and objectives are introduced in section 1.3 and 1.4 respectively. The chapter is concluded with the delimitations, rationale of the study and the assumptions. A final section summarises the remaining chapters of this research report.

1.1 Statement of purpose

This research study examines how events, such as the Covid-19 work-from-home (WFH) policies have influenced cybersecurity behaviour of employees in South Africa. The overarching response has been the introduction of a hybrid working model, which has implications for cybersecurity behaviour within the context of remote work.

This study evaluates employee behaviour when working environments are suddenly affected by work-from-home policies and how an employee's behaviour towards cybersecurity practices transposes to a different location. Furthermore, the study evaluates the key constructs that influence cybersecurity compliant behaviour, while assessing employee's perceptions on behavioural traits,

1.2 Background of the study

The Covid-19 pandemic was an unprecedented event that resulted in drastic measures by world governments to mitigate the infection rate. South Africa was not exempt and based on the recommendations from the World Health Organisation (WHO), initiated work from home (WFH) policies to lessen the spread(World Health Organisation, 2021)

The resulting government strategies (South Africa, 2021), forced organisations to transform their information technology (IT) infrastructure almost instantaneously. As a result, previous office-based employees were forced into a relatively new experience of remote work. While the outbreak of Covid-19 began in 2020, many employers have opted for hybrid working conditions post lockdown. A recent survey by Microsoft (2020)

showed that 88% of leaders at large enterprises in South Africa will adopt a more hybrid way of working permanently.

This has increased the target base for cybercriminals and have removed employees from more robust office security protocols. Information and communications technology (ICT) departments within South Africa organisations had to deliver quick digital solutions to keeps employees connected and retain business processes. Furthermore, these solutions still required confidentiality, integrity, and availability (CIA) of data without the time flexibility to perform an informed risk assessment to mitigate cybercrime as proposed by the National Institute of Standards and Technology (NIST, 2018, p. 20).

Cybersecurity has emerged as one of the most pressing issues and worries of contemporary emergency digitalisation for South African companies, with many instances of information and privacy breaches during lockdown.

Therefore, this study aims to evaluate employee behaviour when working environments are suddenly affected by work-from-home policies and how an employee's behaviour transposes to a different location.

1.2.1 Lasting Cyber Risks introduced by the Pandemic lockdown.

The South African corporate environment was dependent on digital communication to ensure some degree of operational normality during the lockdown. This unfortunately led to a significant increase in cyber-attack according to survey conducted by Accenture (2022). While the official lockdown ceased in February 2022, the statistics reveal an ongoing increase in attacks to employee's devices in the work-from-home (WFH) environment. (Malwarebytes, 2020). This poses a threat to the perimeter security and the unauthorised access of company assets within South African organisations, who are at the risk of being breached.

According to Baz et al. (2021), it is a difficult task to implement organisation's security guidelines and controls on remote working employees. Company security policies required comprehensive modification, and the monitoring of adherence by employees is still a growing concern. The main risk to a company's data security is considered to be

human errors, and most IT teams lack visibility into this employee vulnerability, which is worsened by employee's remote work arrangements (Borkovich & Skovira, 2020).

One of the fundamental requirements for remote working in any corporate environment, is the ability for employees to communicate and share data securely. Therefore, collaboration (Microsoft Teams, Zoom) and file sharing tools, numerous personal devices connecting to the network, increased email and digital traffic, corporate cloud solutions, and similar related changes in the organization may result in data breaches, theft of data, which could cause reputational and financial damage to organisations (Seymour, 2020).

1.2.2. Increased Security Risk from Remote Working

A recent survey by conducted in the United States showed that 58% of employees use personal applications like Gmail and Dropbox, to transmit confidential company information, due to convenience and ease of use (Pham, 2021). Furthermore, remote workers use public Wi-Fi and unsecure access for work related activities. Omorog and Medina (2020) conducted a study in the Philippines to explore cybersecurity awareness in the context of remote work and found that from a sample size of 252 employees, 40% of respondents use public access.

In a South African context, the deficit of cybersecurity awareness is further exacerbated by the constant power interruptions by the national service provider, which sometimes force employees to seek alternate power and network access in the public domain (Public Wi-Fi, coffee-shops, Internet Cafés). A similar predicament exists in Nigeria, where a privileged few have access to high speed internet, and the remaining population rely on the public space and free internet for work related activities (Baz et al., 2021).

Employees working remotely also rely on home Wi-Fi network to connect to their corporate network, due the lack of mobile data coverage during power outages. This may not be secure according to cybersecurity expert's and pose a threat to company data assets (Škiljić, 2020). Furthermore, remote workers may unintentionally share sensitive data over unprotected channels or devices, potentially resulting in data breaches. While most studies reflect on the potential of cyberspace breaches, one of the specific issues in South

Africa is also physical theft. Without the regulated, access controlled physical environment of an office, there is a greater chance that devices containing sensitive data will be physically stolen or lost. Therefore, security measures including passwords management, encryption of local data, and patch management is paramount in securing unauthorised access to physical endpoints (Borkovich & Skovira, 2020).

1.2.3. Post COVID-19 Posture

Globally, the lockdown policies have been mostly overturned, however the aftermath from a cybersecurity perspective and the change to a hybrid culture has certain consequences. While companies have adopted various remote access technologies (Virtual private network (VPN), Multi-factor authentication (MFA)), the unauthorised device access from a perimeter perspective still poses a major security threat (Deo et al., 2021).

A survey study by Bloom (2014), used a sample size of a single organisation, whereby 50% of staff were office bound, and the remaining were forced to a work-from-home. The results found that performance information gathered at the study's conclusion showed that remote workers were not only happier and less inclined to leave their jobs, but also more productive than those that were office bound. South African organisations have seen a similar trend, and some are already opting for hybrid models, while large organisation are almost fully integrated into a permanent work-from-home policy (Microsoft, 2020). The sentiment, therefore, is that a certain degree of remote work adoption decreases operational expenditure in terms of office space and operational expenditure, while increasing productivity and flexibility. Contrary to these benefits, remote work has somewhat increased the vulnerability of employees (Baz et al., 2021).

1.3. Research problem

South Africa has been plagued by an increase in cybercrime and was recently highlighted by Accenture as the third most cybercrime victims worldwide (Accenture, 2022). The resulting financial loss amounts to a considerable R2.2 billion in 2021. Furthermore, Interpol have concluded a report, showing 230 million threat detections in 2021 in South Africa and can be attributed to Covid-19 work-from home policies (INTERPOL, 2021).

A recent report by Tessian (Hancock, 2022) showed that 88% of cybersecurity breaches are due to human error. Furthermore, the fight against cybercrime and the prevention of digital attacks within businesses primarily focuses on technology, but lacks emphasis on understanding human behaviour (Hadlington, 2018).

Various studies on cybersecurity prior to Covid-19 (Han et al., 2017; Ifinedo, 2012; Li et al., 2019) showed that organisational security policies do not work effectively, due to lack of adherence or employees underestimate the information security risks. Furthermore, employers that have provided an adequate level of mandatory information security training by their employees do not necessarily demonstrate greater levels of cybersecurity behaviour, which is exacerbated by remote work. While there are many advantages of remote work, both for the organisation and the employee, the main drawback is the increased exposure to cybercriminals and hackers.

Furthermore, the skilled hackers often concentrate on the value of the data rather than the infrastructure that allows for its access. Remote employees may already access this important organisational data by logging into their work computers from home, usually with more access than is necessary (Borkovich & Skovira, 2020). Therefore, if a hacker can access a single user account that is vulnerable, it provides an unsolicited access to the organisation's network and data assets.

The overarching question is how has cybersecurity behaviour in South Africa manifested during work-from-home policies? What are the determinants that force correct cybersecurity protection motivation in adherence to organisational security policies? How does an individual risk assessment and self-efficacy inspire correct cybersecurity behaviour? Therefore, this study aims to evaluate employee behaviour when working environments are suddenly affected by work-from-home policies and how an employee's behaviour transposes to a different location.

1.4. Research objectives

This purpose of this research study was to examine how extraordinary events, unprecedented lockdown rules and remote or hybrid working models affect employee security behaviour in South African. The objective of this research study was to determine

the key factors that influence cybersecurity compliant behaviour while working remotely and is captured below:

Research objective 1

To examine the human aspect of cybersecurity compliant behaviour while assessing employee's individual behaviour traits in a remote working environment

Research objective 2

To investigate and assess the key factors that influence positive cybersecurity compliant behaviour while working remotely, incorporating past literature on office-based cybersecurity behaviour.

1.5. Rationale

Work-from-home (WFH) has been a long-awaited expectation globally due to the continuous advancement in information technology (IT), and the exponential growth of data access even in developing countries. The stagnant adoption of organisational policy regarding remote work is evident globally (Furnell & Shah, 2020) and could be attributed to various reasons, however the recent pandemic has abruptly changed the status quo. The resulting effects has seen an increase in cybercrime and South African's have been a target for cybercriminals looking to exploit both personal and corporate weaknesses in data and information protection.

This study aimed to add to the exiting literature of Cybersecurity Compliant Behaviour and while there have been many studies prior to the Covid-19 Pandemic (Safa et al., 2015; Torten et al., 2018), these were based in office environments where constant evaluation and training was a prerequisite and the main criteria for correct employee cybersecurity behaviour.

This research also aims to contribute to the literature as a result of the Covid-19 lockdown and the subsequent hybrid working model to serve as a resource to supplement leadership initiatives in South Africa in the context of cybersecurity. The benefit of this study is to provide South African business leaders with a foundation of understanding how employee

cybersecurity behaviours change without the constant engagement from peers and management regarding cybersecurity in an office environment.

1.6. Delimitations

The context of this research study is to provide insight of cybersecurity behaviour during work-from-home or hybrid working models. Therefore, the criteria for survey participation are limited to respondents that are subjected to these specific working environments. Furthermore, it excludes those that are considered as full-time office-based employees, particularly employees that are front-line staff that are exempt from work-from-home models (law enforcement, medical staff).

Additionally, from the device perspective, work-from-home participants are limited to performing day-to-day tasks associated to their work requirements using either a desktop or laptop devices. Mobile handsets will not be considered as part of this study, which may be the case for telemarketing and call-centre employment.

1.7. Definition of terms

Cybersecurity is the practice of preventing unauthorized access to networks, devices, and data as well as the practice of preserving the confidentiality, integrity, and accessibility of information (Craigen et al., 2014).

Cyber-Crime refers to any criminal offence that is involves the use of electronic communications or information systems, including any device or the Internet (Gordon & Ford, 2006).

Multi factor authentication - To access a resource like an application, an online account, or a VPN, the user must submit two or more verification factors in order to access the required internal network (Ometov et al., 2018).

Remote work, often known as working from home or telecommuting, is work performed away from a regular office setting. The idea behind remote work is that employees can do everyday duties and projects without having to travel to an office every day.

VPN - A system whereby encryption is used to create a secure, seeming private network over a public network which is usually the internet (Ferguson & Huston, 1998).

1.8. Assumptions

The assumption is that respondents that fit the criteria of work-from-home policies, have received some form of security training from their employees or have gathered security knowledge in their personal capacity. It is also presumed that the employee has accepted the remote or hybrid work arrangement and is adequately prepared to embrace the change in working conditions.

Furthermore, the assumptions are related to the government-enforced lockdown that South Africa implemented to restrict people's movement and mitigate the virus spread, have forced employees to adopt work-from-home business policies. Furthermore, respondents have answered the questions as honestly and possible.

1.9. Chapter Outline

This research report consists of six main chapters. The first chapter provided context of the research study, highlighted the research problem which yielded the design of the main research objectives. Based on the body of literature, the research questions formed the basis for the hypothesis.

Chapter 2: This chapter offers a review of the existing literature and analyses the problem statement and underlying constructs. Furthermore, established theoretical frameworks were evaluated within the cybersecurity domain, which led to the derivation of the conceptual framework to guide the research design and data collection presented in chapter 3. In addition, it explains the relationship of employee behaviour.

Chapter 3: The chapter presents the research design and the methods of data collection. It further presents the research questionnaire, sampling and steps undertaken to ensure quality of data (reliability and validity). In addition, it describes the ethical consideration for the research report. Lastly, to ensure an alignment of framework versus the analysis. This chapter explains the statistical techniques utilizes in the data analysis process.

Chapter 4: This chapter offers the empirical results gathered from the research instrument, and the subsequent statistical results from SPSS version 28. It begins with the descriptive statistics, highlighting key information for further data analysis. Thereafter presents the Exploratory Factor Analysis (EFA), followed by the reliability and validity of both conceptual and empirical constructs. After the model is updated, the regression results are presented with the hypothesis test results.

Chapter 5: This chapter uses the conceptual and theoretical framework suggested in Section 4.13 to interpret and analyse the empirical findings reported in Chapter 4. Together with previous research and actual outcomes, the findings pertaining to each hypothesis are explored and clarified. Lastly, a summary is presented to reflect the conclusion of the findings.

Chapter 6: This chapter presents the recommendations for organisations and researchers based on the findings of the study. It further the explains the limitations and provides a final conclusion to this research report.

2. LITERATURE REVIEW

This chapter aims to present three overarching objectives. Firstly, to review the literature to better comprehend the research problem, secondly, to establish a possible gap in knowledge and lastly, to develop a conceptual framework underpinned by established theoretical frameworks. The introduction to the literature is followed by work-from-home considerations and the typical behavioural conditions that motivate cybersecurity compliant behaviour.

2.1. The Human Aspect of Cybersecurity

Over the past two decades, cybersecurity has been viewed from a perspective of protecting networks and information assets. According to the European Union Agency for Cybersecurity (ENISA, 2021), this definition should be expanded to behavioural and socio-economic concerns, and how this affects an organisation's cybersecurity strategy.

Covid-19 and the resulting lockdown policies resulted in a national emergency, forcing a large percentage of the South Africa workforce to adopt a WFH culture. With this drastic change, many organisations looked to their IT departments and suppliers to provide quick solutions to mitigate security risk, opting for multi-factor authentication (MFA), Virtual Private Networks (VPN), encryption and secure communication tools for their employees (Abukari & Bankas, 2020; Borkovich & Skovira, 2020). While these methods are proven for initial access, the threat of the end device (Laptop or desktop) remains, as hackers can use this access without the employee's knowledge.

A recent UK study by Furnell and Shah (2020), examined the WFH culture and the underlying evidence of organisational policies to facilitate home or mobile working. Most companies had generic rules in place that was integrated for traditional office environments. The results also showed that over 75% of companies did not have a have a definitive cyber security policy in place for WFH environments and relied on employee's good judgment and initiative to objectively make the correct security decisions.

Human error has since been the major cause of cybersecurity breaches (Hancock, 2022), and while organisations have opted for the latest technology in encryption and security,

hackers and cybercrime are targeting the end user to gain access to company intellectual property (IP) and customer information. Evidently, when it comes to home environment, workplace security procedures like notifying the IT Department of questionable emails, spam, videos, texts, invitations, links, and attachments, WFH employees frequently have security amnesia (Borkovich & Skovira, 2020).

2.1.1. Work from Home/Hybrid working.

The pandemic lockdown instituted by the South African government highlighted the need for work-from-home policies. South African organisations were expected to retain the normality of productivity, effectiveness and collaboration while ensuring the protection of data and influence the adherence of correct cybersecurity behaviour (Georgiadou et al., 2022).

Furthermore, the lockdown ended in 2021, but the hybrid model, according to a recent survey by Microsoft, 88% of leaders at large enterprises in South Africa will continue to adopt a more hybrid way of working permanently (Microsoft, 2020). The data also showed that more long-term changes in working practices are already visible, with a sizable majority (82%) of businesses having established policies regarding remote work. Senior leaders recognize the possibility to preserve efficiency improvements while also enhancing employee engagement. Furthermore, the data also showed that 76% of increased productivity in a remote setting, and believe it to be an effective strategy for keeping their best employees (Microsoft, 2020; Shen et al., 2020).

2.1.2. Cybersecurity Compliant Behaviour

South African organisations deal with information and personal data on a regular basis and is fundamental for daily operations. The recognised value inherited from this data (McAfee & Brynjolfsson, 2012) must be protected and measures are generally taken to survive an attack. Cybersecurity behaviour is essentially the measures adopted by the employee to further enhance information security. Previous studies have indicated that the main cause of information breaches are as a result of employee non-conformance to security policies (Beautement et al., 2008; Hadlington, 2018).

Cyber hygiene as explained by Kalhoro et al. (2021), is a composition of behaviours that promote positive cybersecurity compliant behaviour. Essentially, this behaviour requires employees to gather knowledge about cybersecurity, either initiated by their employers or in their personal capacity. Therefore, in a South African context, this knowledge provides a foundation for early detection of threats and managing day-today work tasks while in a remote working environment. Employees working remotely may have the intention to comply with information security policies, but are still considered to be the weakest link (Alsharida et al., 2023; Hadlington, 2018; Hancock, 2022; Hanus & Yu, 2016; Shropshire et al., 2015).

2.2. Definition of Key Constructs

2.2.1. Employee Threat Assessment

The term "threat" refers to the probability and severity of a dangerous event or consequence. Within the context of a WFH environment, it describes the possibility of either personal or organisational information loss resulting in reputational or financial damage (Safa et al., 2015).

The Protection Motivation Theory (PMT) (Rogers, 1975) has been used extensively in previous cybersecurity behavioural studies (Hanus & Yu, 2016; Safa et al., 2015; Torten et al., 2018), and the theoretical framework provides an initial appraisal by an employee based on the facts and the subsequent interpretation of the threat. Therefore, PMT highlights two processes, threat, and coping appraisal that, in the context of this study can be used to determine behaviour. The threat appraisal comprises two key constructs, specifically perceived severity and perceived vulnerability (Rogers, 1975).

According to Hanus and Yu (2016), desktop and mobile security presents a significant threat to information security, and irrespective of the capital invested within the organisation from a technological and physical perspective, it is only as strong as the weakest link. The more an individual is concerned about a potential threat, the likelihood of reacting to mitigate any harmful causality (Anderson & Agarwal, 2010).

To capture the influence of employee threat assessment in this study the two factors below will be utilised within the realms of Perceived or Threat Severity and Perceived Vulnerability

2.2.1.1. Threat severity

Threat severity is the magnitude at which an employee perceives the negative incident, should it occur. The construct for the purposes of this study will be referred to as perceived severity. Perceived severity refers to the potential for a negative event, while perceived vulnerability is the magnitude of the probable consequence when the negative outcome occurs (Hanus & Yu, 2016). Employees are more likely to take part in information security training offered by their employers or introspectively learn computer security procedures if they believe that a security threat will result in major losses and serious disruptions at their employer (Li et al., 2019).

An employee won't be alert to the seriousness of information crime if they don't think they are dealing with information security crime (Herath & Rao, 2009). Employee security knowledge, attitudes, and training provided by their businesses, significantly influence how seriously people perceive information security. A recent study by Alsharida et al. (2023) noted that many of behavioural studies in cybersecurity between 2011 and 2021, perceived severity was one of the most common independent factors in all studies, which confirms the use of the PMT theory for cybersecurity related behavioural research. Therefore, this construct is captured in the hypothesis:

H1: Perceived severity has a positive influence on Cybersecurity Compliant Behaviour.

2.2.1.2. Perceived vulnerability

Employee perception of vulnerability refers to how much they perceive a cyberattack incident's threat and the need for preventive measures and activities (Vance et al., 2012). Employees are less vulnerable in preventing new cyber-attack occurrences if they have prior cybersecurity experience in managing information and access breaches (Torten et al., 2018).

Furthermore, employees in a remote work setting are just as susceptible if not more, to security risks as users in an office environment. While there are several causes of this susceptibility, a study by James et al. (2013) on the antecedents of security practices in the general public domain, posits that a lack of knowledge and personal initiative are the main determinants for adhering to correct security practices. Similarly, a study on cybersecurity awareness conducted on 200 Small and Medium Enterprises (SMEs) by Wong et al. (2022) theorises that employees whose perceive their vulnerability as high, will ensure the that they seek necessary training, research methods or seek expert advice to mitigate these vulnerabilities. Therefore, this construct is captured in the hypothesis:

H2: Perceived vulnerability has a positive influence on Cybersecurity Compliant Behaviour.

2.2.2. Employee efficacy

The PMT framework consists of a coping appraisal, which describes an individual's evaluation of his or her capacity to prevent the potential loss or damage resulting from the threat (Rogers et al., 1983). For this study, the coping mechanism can be categorised in two components – Response Efficacy and Self-Efficacy.

Torten et al. (2018) conducted a quantitative study to examine impact of security awareness amongst IT professionals in Australia, The analytical results from 408 respondents demonstrated that the constructs of response efficacy and self-efficacy provided the strongest influence on security behaviour. The results also indicated that the corrective actions by users inferred a positive relationship to the coping appraisal. The outcome is consistent with a similar study by Hanus and Yu (2016), utilising the PMT theory to examine the impact of security awareness on desktop security in the United states of America (USA). This sample, however consisted of 241 non-IT professionals, yielding a comparable result. The implications of both studies showed a common outcome of these constructs demonstrating the usefulness to determine behavioural intentions (Maddux & Rogers, 1983) within a cybersecurity context. Therefore, the two facets of employee efficacy are captured below as Response Efficacy and Self-Efficacy.

2.2.2.1. Response Efficacy

This construct describes the person's perception of the advantages of the actions they took (Rogers, 1975). In the context of this study, it alludes to the actions that employees will undertake to pre-empt any security threats, to mitigate data breaches. In addition, is further complies with correct security conscious behaviour for identifying potential threats to the organisational data assets.

Response efficacy is regarded as a distinct personality trait that can be effectively, and a recent study by Shappie et al. (2020) examined the relationship between behavioural intentions and specific cybersecurity behaviours. According to the findings by Wong et al. (2022), employees are more likely to adopt suitable actions when their perception of response efficacy increases. As a result, organisations must promote training and assistance to their employees in order for them to correctly use the technology and enhance their response efficacy. Therefore, this construct is captured in the hypothesis:

H3: Response-efficacy has a positive influence on Cybersecurity Compliant Behaviour.

2.2.2.2. Self-efficacy

Self-efficacy as a construct, places emphasis on the person's capability or assessment and the personal capacity to carry out the appropriate behaviour (Rogers et al., 1983). It refers to the abilities and precautions required in the context of this study to safeguard information and adhere to correct cybersecurity behaviour. It has been demonstrated that self-efficacy has a major impact on a person's capacity to carry out or perform a task (Donalds & Osei-Bryson, 2020).

Rhee et al. (2009) indicated that self-efficacy is a major influence on cybersecurity behaviour. The study focused on 415 business graduates and found that the adoption level of security software and tools was higher in graduates that had a high self-efficacy, and in contract, those with low self-efficacy engaged in fewer mitigating actions towards protection of assets.

In this study, therefore, this construct aims to gather an employee’s capability to follow recommended behaviours and best practices for cybersecurity. Therefore, Self-efficacy

in the context of this study of remote work, is a key component that promotes security conscious behaviour and is captured in the hypothesis below:

H4: Self-efficacy will have a positive influence on Cybersecurity Compliant Behaviours

2.2.3. Attitude

Attitude is defined as the individual's positive or negative feelings toward engaging in a specified behaviour (Ajzen, 1985). For this research, attitude represents an employee's attitude towards acceptable cybersecurity behaviour.

Cybersecurity behaviour can change based on an employee's attitude, and according to Ifinedo (2012) , the composition of attitude, subjective norms and self-efficacy within the cybersecurity domain has a positive relationship on cybersecurity compliance. The study posits that attitude alone, plays a vital role in influencing behavioural change, and many factors like skills, training and self-learning can further impact change.

A similar study by Tam et al. (2022) examined the factors that influence employees to follow security policies. The results demonstrate that a favourable attitude towards cybersecurity compliance will encourage employees to administer the corrective actions. Safa et al. (2015) also asserted that cybersecurity awareness motivates users, however lack thereof, promotes a resistance to simple security administrative actions.

According to the Ajzen (1991) the construct of attitude is an overarching sentiment of liking or disliking a specific behaviour. In the context of this research study, it describes the degree to which the person believes that undertaking security measures is a desirable action. A study by Hadlington (2018), posits that most employee's attitude towards cybersecurity reflect as negative in an office environment, as they believe that protection is maintained by their organisations. Therefore, this study aims to show the positive effect of attitude towards correct cybersecurity behaviour in a WFH setting, and is captured in the hypothesis below:

H5: Employee's positive attitude will have a positive influence on Cybersecurity Compliant Behaviour.

2.2.4. Subjective Norms

Various studies have applied the theory of planned behaviour (Anderson & Agarwal, 2010; Ifinedo, 2012; Tam et al., 2022) and while organisations have taken technological measures to protect their assets, employee motivation to comply with policies is still a major consideration.

Subjective norms (SN) are a person's opinion of what people in their social and work environment value about a particular conduct. It also is a behavioural predictor and makes reference to the idea that normative views are those formed as a result of social pressure (Ajzen, 1985). Generally, in an office environment, South African corporates ensure several stimuli to promote correct security behaviour. These include visual posters, face-to-face seminars with security experts, and training, however studies show that influence of cybersecurity compliant behaviour will emanate from peers within their organisation. -Supervisor, Department Head, Managers, and peers (Safa et al., 2015). A study by Anderson and Agarwal (2010) regarding home computer safeguarding, posits that subjective norms is a strong predicator of protecting computers from unauthorised access. Similarly Ifinedo (2012) investigated security policy awareness amongst a sample of 124 employees, and noted that subjective norms was a significant determinant of security behaviour. Therefore, the hypothesis below captures this phenomenon:

H6: Employee's positive subjective norms will have a positive influence on Cybersecurity Compliant Behaviour.

2.3. Analytical Framework

The usefulness of the frameworks and the circumstances in which they can be used are covered in this section. The use of this specific framework to this research project is then discussed. By investigating the determining elements that affect Cybersecurity Compliant Behaviour based on fear and threat appraisal, this section of the study explains the theoretical frameworks that earlier studies have employed to explain and forecast employee behaviour and attitude on effective security behaviour.

2.3.1. Theoretical Frameworks of Cybersecurity Compliance

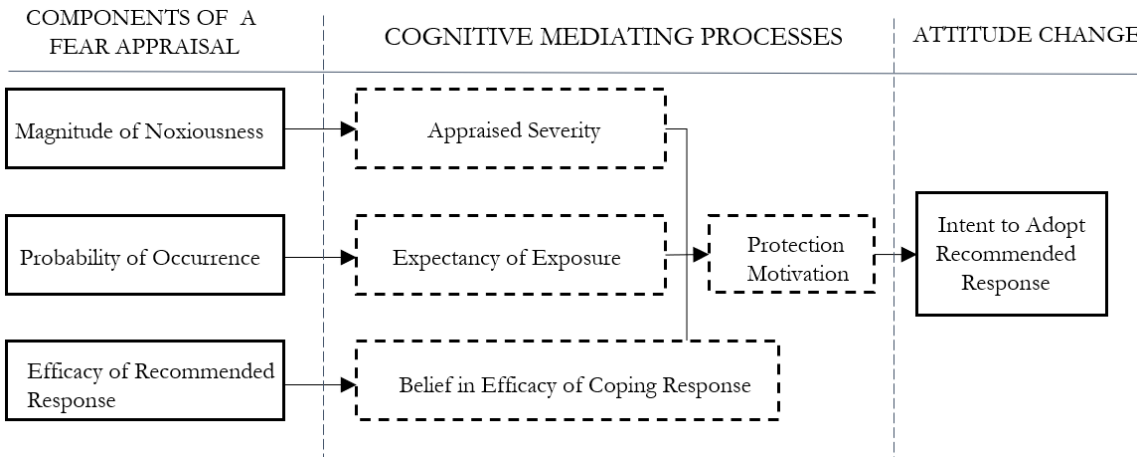
Cybersecurity compliance and the overarching determinants that influence the correct employee behaviour has been widely studied over the past two decades, however this context was based on a procedural training by organisations (Li et al., 2019; Tam et al., 2022). The physical setting is generally based within an office environment, where constant communication by an employer and peer engagement propagates correct cybersecurity behaviour. This study aims to evaluate the behavioural intention when working environments are suddenly affected by work-from-home policies and how the behaviour transposes to a different location.

2.5.1.1. Protection Motivation Theory

Protection Motivation theory (PMT) shown in Figure 1, was developed by Rogers (1975) with an initial hypothesis to forecast people's involvement in health risk prevention, however the effectiveness was further realised within the cybersecurity domain. Over the past two decades, various cybersecurity behavioural studies had instituted and established the applicability of PMT (Ifinedo, 2012; Li et al., 2019; Torten et al., 2018).

According to the model, three factors - the impact of the event, the likelihood that it will occur, and the efficacy of the individual in defending against the possible occurrence. These three elements lead to the fear appeal. An individual's behaviour is directly impacted by fear, and the perceived harm that could occur without intervention. Both the threat assessment, and the coping evaluation are the sources that drive an individual to defend and exhibit a protective response. An individual's judgment of the degree of danger offered by a hazardous event is referred to as a threat appraisal. Furthermore, if an event is not appraised as severe, then it is unlikely or if nothing can be done about it, then protection motivation is not triggered, and therefore no change in behaviour (Rogers et al., 1983). The higher the level of fear, the more the attitude changes towards the adopting the specific behaviour.

Figure 1: The Protection Motivation Theory Model



2.5.1.2. Theory of Planned Behaviour

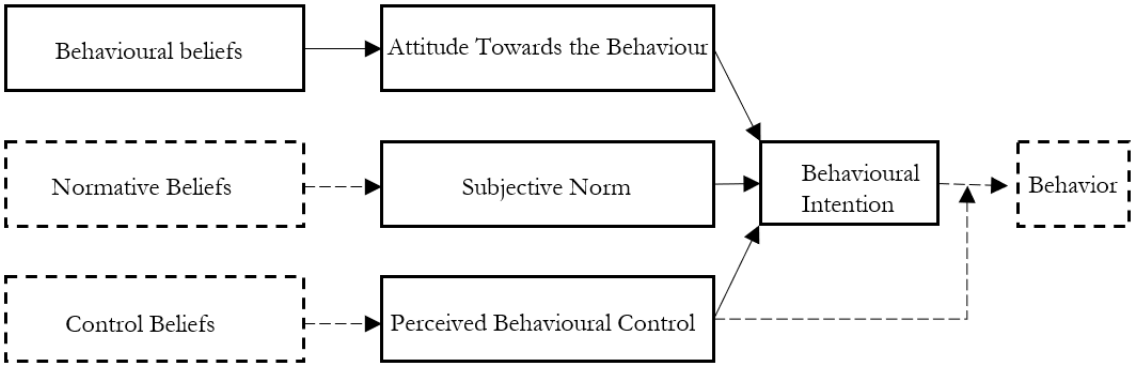
The Theory of Planned Behaviour (TPB) model presented in Figure 2, describes the relationship between intrinsic belief and the subsequent behaviour (Ajzen, 1985). Ajzen enriched the Theory of Reasoned Action (TRA) by adding the perceived behavioural control (PBC) construct. TPB theorises that a person is more likely to engage in a behaviour if they have a positive attitude toward it (Attitude) and believe that other individuals desire them to do so (Subjective Norms), and motivated by this, they are more inclined to follow through on the decisions.

TPB has been widely used in previous cybersecurity research studies (Ifinedo, 2012; Safa et al., 2015; Tam et al., 2022). Furthermore, Safa et al (2015) explored the key constructs on TPB within a cybersecurity awareness framework, while utilising independent variables of organisational policy, Information security awareness, and overall employee experience. Although this study was conducted pre-Covid, the application of TPB provides a relevant platform for cybersecurity awareness perception.

An individual's favourable or negative feelings about partaking in a particular conduct are referred to as their attitude. It captures the attitude regarding cybersecurity compliance in a WFH environment. Subjective norms reflect how an individual believes that other individuals who are significant to them feel about a particular conduct.

Perceived behavioural control, the third element of TPB, refers to self-efficacy and pertains to a person's perception of the ease or difficulty of performing a specific behaviour.

Figure 2: The Theory of Planned Behaviour Model

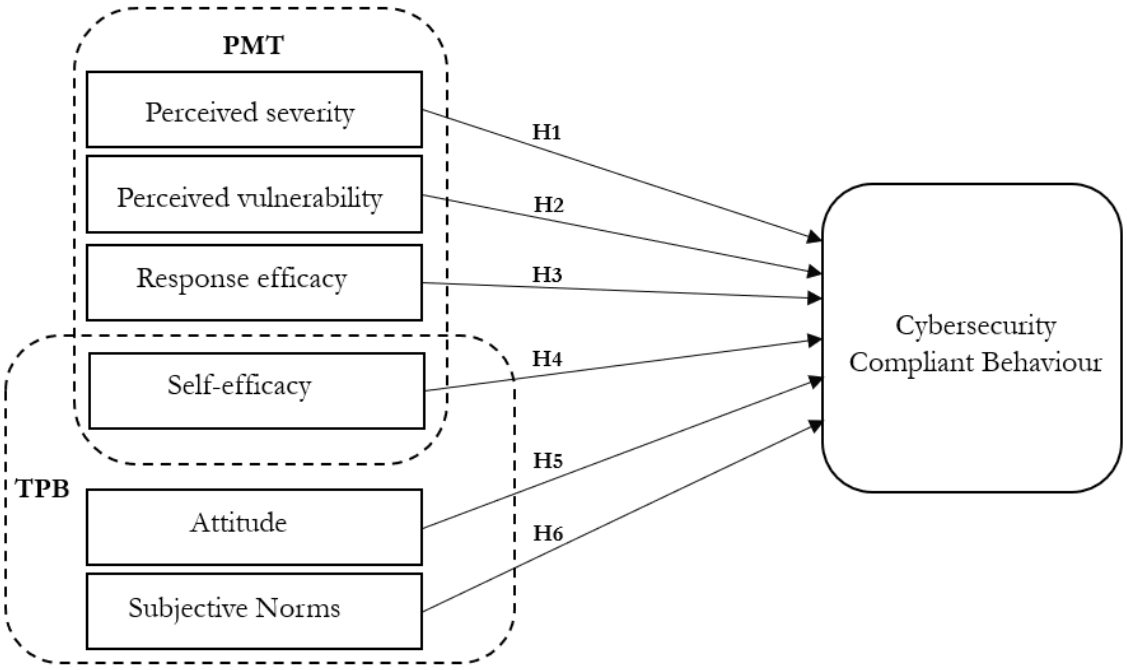


2.3.2. Conceptual Framework

The conceptual framework represented in Figure 3, was adapted using a combination of two established models (PMT and TPB). The six predictor variables (*Perceived severity, Perceived vulnerability, Response Efficacy, Self-efficacy, Attitude, and Subjective Norms*), provides a foundation to capture the perceptions and actions of employees within a work-from home environment, based on previous literature. This new experience for South Africans has been a product of the recent Covid-19 lockdown policies and some form of hybrid working has ensued for most corporate entities (Microsoft, 2020; Shen et al., 2020) due to its financial and employee psychological benefits.

The threat appraisal and coping appraisal are the two appraisal processes that make up the PMT model. When employees are faced with potential cyberattacks, the perceived severity and perceived vulnerability are considered in the threat assessment. Employees are more likely to actively learn computer security procedures or take part in information security training offered by their employers, if they believe a security threat will result in major personal losses or and serious disruptions to their employer (Li et al., 2019). This is a fairly new framework so the necessary statistical analysis will be conducted to ensure reliability, validity in predicting "*Cybersecurity Compliant Behaviour".*

Figure 3: Research Model - Adapted from the Protection Motivation Theory and the Theory of Planned Behaviour



2.4. Conclusion of Literature Review

Covid-19 and the resulting changes to normality have caused enormous challenges for South African businesses, and while the primary focus was on economic, social, and psychological effects, one cannot ignore the impact on cybersecurity. Enforcing security policies and controls on a remote workforce is a difficult task and some businesses have had to allow the use of personal devices for work related tasks (Deo et al., 2021).

South African businesses may have made investments in security technologies and implemented corresponding procedures; however their employees will always be the chink in the armour of cybersecurity (Deloitte, 2020). Covid-19 and the subsequent hybrid mode has permanently altered the attitude towards remote work, and therefore this study aims to find a correlation between employee behaviour and the influencing factors that encourage correct security decisions in a remote setting. The constructs of perceived severity, perceived vulnerability, response efficacy, self-efficacy, attitude, and subjective norms have been identified as the determinant to correct security behaviours and are captured in the hypothesis below.

H1: Perceived severity has a positive influence on Cybersecurity Compliant Behaviour.

H2: Perceived vulnerability has a positive influence on Cybersecurity Compliant Behaviour.

H3: Response-efficacy has a positive influence on Cybersecurity Compliant Behaviour.

H4: Self-efficacy will have a positive influence on Cybersecurity Compliant Behaviour.

H5: Employee's positive attitude will have a positive influence on Cybersecurity Compliant Behaviour.

H6: Employee's positive subjective norms will have a positive influence on Cybersecurity Compliant Behaviour.

3. RESEARCH METHODOLOGY

The chapter presents the research approach and design in Section 3.1 and Section 3.2 respectively. The methods of data collection supplemented by the research instrument are explained in Section 3.3. It further presents the population and sampling and steps undertaken to ensure quality of data (reliability and validity). In addition, it describes the ethical consideration for the research report. Lastly, to ensure an alignment of framework versus the analysis. Section 3.5 explains the statistical techniques utilizes in the data analysis process.

3.1. Research Philosophy

A research paradigm is a collection of widely recognized research practices, attitudes, and procedures that guide and shape researcher's conceptualization, conduct, and communication of their study(Saunders et al., 2019). The philosophical assumptions that underpin this research are founded on a post-positivist philosophical viewpoint that is scientific in character and often employs a quantitative method(Creswell & Guetterman, 2018) The benefit of this technique is its objectivity in data analysis and interpretation. Furthermore, deductive logical thinking allows for the utilization of present rules, assumptions, discoveries, and theories to deduce a conclusion, as well as the generalization of facts(Saunders et al., 2019).

3.2. Research approach

To achieve the goals and objectives of this research study, a cross-sectional research design was used as a component of a quantitative research approach (Schindler, 2019). A structured, closed questionnaire was developed and adapted using the existing literature and was distributed online to respondents. Convenience, low administrative expenses, and increased accessibility for participants across a wider geographic range were the benefits of electronic distribution (Kumar, 2019). The collected raw data was transformed and prepared for analysis using the Statistical Package for Social Sciences (SPSS) V28. The results were thereafter referenced against the research objectives and their corresponding hypotheses to get insights about employee cybersecurity behaviours in a WFH culture.

In a comparable study, Torten et al. (2018) examined the impact of security awareness using a quantitative approach. The findings of the research described various factors that influence security conscious, desktop behaviour. The study emphasized that it is critical that employees are aware of risks and organisational policies.

Similarity, Hanus and Yu (2016) employed a quantitative approach examining desktop security awareness with a sample size of 241 respondents, which was large enough to effectively test all the hypotheses in the research model. This research study will benefit from the similar approach by granting access to a larger group of employees in a variety of geographic locations within South Africa to extract greater insights.

3.3. Research design

The research design, simply outlines all planned steps to fulfil the research objectives (Schindler, 2019, p. 71). Similarly Kumar (2019) suggests that the research design provide guidance on data collection (questionnaire), selection of participants (sample) and the data analysis, leading to the final presentation of the results.

For this research report, a cross sectional, quantitative design was used, based on previous studies and the evaluation of the current limitations. This design provides a snapshot of the overall status regarding a phenomenon at a single point in time (Kumar, 2019). The data collection and research instrument was derived to capture the factors that influence cybersecurity compliant behaviour, and was adapted from prior studies by Hanus and Yu (2016), Ifinedo (2012), Li et al. (2019) and Safa et al. (2015). In addition, Appendix A(Table 46) provides a detailed derivation of the research instrument, including the references to previous research studies.

Previous studies by Tam et al. (2022) and Ifinedo (2012) used a cross-sectional approach to explore the key determinants of conducive cybersecurity practices, and found a positive relationship to behavioural traits. The approach is therefore, guided by the research objectives, existing literature and associated external factors including time constraints, no funding requirements and sample requirements within various employers in South Africa.

3.4. Data Collection and the Research Instrument.

A research study's data collection procedure involves gathering information from all relevant sources in order to address a phenomena, or research problem (Kumar, 2019). This research used an online closed questionnaire that is designed to extract information guided by the research objectives and the conceptual framework. Appendix A provides a copy of the data collection instrument.

With the use of QUALTRICS, the final questionnaire was accessed via a Uniform Resource Locator (URL) which is a link to the questionnaire. To invite participants, the online survey link was sent by email and many social media channels (Outlook, WhatsApp, and Facebook). The raw data result was downloaded for analysis and password-protected online, and on a local computer.

This research employed an online closed questionnaire that is designed to gather information guided by the research objectives and the conceptual framework. The advantage of using closed questionnaires (Schindler, 2019) is that respondents are given fewer options for possible answers, which eliminates the possibility of response variability. The process of gathering and analysing information about specific variables in a planned, methodical way is known as data collection (Bairagi & Munot, 2019).

The research instrument consisted of 35 items, where the first six items captured demographic data, and confirmation of criteria from respondents to fit the research study. An early item within the flow of the research instrument represented the status of the respondents current working environment, which is fundamental for the study. Thus, the question below alleviated any unusable or missing data and limited the responder's time by exiting the survey if this criterion was not met.

"During Lockdown, I was offered the opportunity to work from home via remote access?"

"I am currently working from home or spend a part of my "work week" at home."

The seven constructs including the dependent variables utilised 29 items based on a Likert scale, ranging from *strongly disagree* to *strongly agree*. The various scales use in this study was adapted from previous literature and the sources per scale are available in Appendix A (Consistency Matrix).

In a similar study by Li et al. (2019) which examined the determinants of cybersecurity police awareness , a closed questionnaire was utilised. The study was able to gather short customer responses as well as data on the respondent's sociodemographic traits during a limited timeframe.

Thus, the data collection and research instrument (Table 1) was derived to capture the factors that influence cybersecurity compliant behaviour, and was adapted from prior studies by Hanus and Yu (2016), Ifinedo (2012), Li et al. (2019) and Safa et al. (2015)

Table 1: Summary of Items per Construct

OBJECTIVE	CONSTRUCT	DATA SOURCE	VARIABLE
Cybersecurity Threat Assessment	Perceived severity	Q.22 - Q.25 (Likert)	Independent Variable
	Perceived vulnerability	Q.18 - Q.21 (Likert)	Independent Variable
Employee Response efficacy	Response efficacy	Q.30 - Q.33 (Likert)	Independent Variable
	Self-efficacy	Q.14 - Q.17 (Likert)	Independent Variable
Attitude	Attitude	Q.8 - Q.13 (Likert)	Independent Variable
Subjective Norms	Subjective Norms	Q.26 - Q.29 (Likert)	Independent Variable
	Cybersecurity Compliant Behaviour	Q.32 - Q.36 (Likert)	Dependent Variable

3.5. Population and sample

3.5.1. Population

The population refers to the complete group of volunteers that are accessible before starting the data collection and is essentially a subset of the universe. (Bairagi & Munot, 2019). The target population for this research consist of employees in the corporate sector that work in South Africa and were subjected to work-from-home frameworks within their organisations. This will be further constrained to employees who use a mixed work-home style, in which some of their productive time is spent at home that have access to their organisations internal data framework via a desktop or laptop. The target population for the distribution of the questionnaire were people living in the various cities within South Africa (Eastern Cape, Gauteng, KwaZulu-Natal, Limpopo, Mpumalanga, Northern Cape, Northwest, and Western Cape).

3.5.2. Sampling method

Kumar (2019) defines sampling as a process of selecting a subset of respondents from a larger group of respondents. The sample will be deduced from the South Africa corporate sector with a prerequisite of an adopted WFH culture. According to Schindler (2019), there are two main types of sampling methods. probability and nonprobability sampling.

Ifinedo (2012) investigated the security policy compliance in Canada to ascertain the factors that influence information systems security policy (ISSP) compliance behavioural intention. The study used a quantitative approach using non-probability convenience sampling; therefore, this study adopted the similar sampling method.

This research focused on the approach of nonprobability sampling as the sampling designs are used when the number of elements in a population is either unknown or they cannot be individually identified (Kumar, 2019). In addition, the proposed convenience sampling will be used, as it provides a low-cost and time efficient technique.

3.5.3. Sample

A total of 186 replies were obtained from the roughly 400 questionnaires that were distributed via electronic channels. Kumar (2019) suggest that a response rate of 50% is adequate. The response rate of the online survey in this study was approximately 47%, which is close to the acceptable value. The online questionnaire was opened for 10 weeks, however due to the snowballing effect it is difficult to estimate a final response rate.

Earlier studies that investigated related research problems have successfully used a similar or larger samples sizes. Ifinedo (2012) investigated security conscious behaviour with a sample size of 124 respondents and the study indicated an appropriate sample using both theoretical frameworks (PMT and TPB). A similar study by Li et al. (2019) examined the impact of cybersecurity awareness amongst American employees utilising the PMT theory , and yielded useful results with 579 respondents, while Tam et al. (2022) had similar results with 196 respondents. The target population comprised of comparable demographics proposed and included working-class adults from different geographic locations that were subjected to a work-from-home environment.

3.5.4. Sample size

According to Pallant (2009), the sample size of a study can inhibit generalisability. Therefore, this study was based on prevalent suggestions in literature regarding the sample size versus the number of variables in the model. Furthermore, Field (2013) suggest 10-15 cases per variable, while Tabachnick and Fidell (2007) posits that a ratio of 20 case per variable will ensure robustness. Therefore, the online questionnaire was opened for a period of 10 weeks ensuring that the final sample size met this criterion.

3.6. Data analysis strategies and interpretation

Data analysis and the statistical evaluation forms a fundamental step in determining final research findings, support hypotheses and will give credibility to research methodologies (Bairagi & Munot, 2019). The statistical methods include a selection of suitable measures or parameters and analysing data for drawing reliable conclusions. This study will consume some of the establish measurements, used by Torten et al. (2018) who studied the impact of information security in Australia.

The data collected post ethics approval was initially uploaded into the SPSS V28 software. After data entry, the information be cleaned and coded to prepare for data analysis.

3.6.1. Statistical Assumptions

In multi regression analysis, there are a few assumptions regarding the data, that could affect the interpretation of the model. To ensure the validity and accuracy of the study, it is critical to carefully analyse these assumptions before utilizing statistical methods (Pallant, 2020). Furthermore, it is critical to assess if these assumptions are valid for the specific data being analysed and to explore alternate methodologies if assumptions are breached (Pallant, 2009). It is thus necessary to address the assumptions of each of these statistical approaches in order to build an accurate representation of the model (Field, 2013).

3.6.1.1. Outliers

Outliers, in the data are values that are much lower or higher than the other scores (Pallant, 2009). According to Field (2013), outliers can cause the model to be influenced because they affect the values of the estimated regression coefficients. Outliers are extremely sensitive in multiple regression, so the first step was to evaluate the data to address the presence of any outliers. This was done by utilizing the Regression Standardized Residuals statistics on SPSS to confirm that the ranges fall between the advised range (between -3.29 and +3.29), as proposed by Field (2013). Furthermore, the graphical representation of the resulting histogram was evaluated for outliers, by checking the tails of the distribution and the presence of any values outside of the advisable ranges. The full analysis is presented in chapter 4, which indicates the presence of two outliers. After the removal of the two outliers. the Regression Standardized Residuals and histogram was recalculated to ensure the outliers were addressed prior to the regression analysis.

3.6.1.2. Multicollinearity

Multicollinearity is the relationship between the independent variables when they are highly correlated (Daoud, 2017). Multiple regression is not conducive to multicollinearity and contributes to biased and unreliable outcomes of the results. With the presence of multicollinearity, there are a few options to correct the model, as suggest by Field (2013) and Pallant (2009). Inaccurate variances and unstable estimations due to collinearity or multicollinearity have an impact on confidence intervals and hypothesis testing. According to Field (2013), if issues of multicollinearity occurs, there is no statistical reasons to exclude one independent variable over another, and Pallant (2009) suggests that combining the variables to form one single composite variable can be introduced to address any multicollinearity issues.

In this study, collinearity statistics included assessing the values of the Condition Index (CI), Variance inflation factor (VIF), Tolerance, and Variance proportion (VP) to determine the presence of multicollinearity (Pallant, 2009). The full analysis is presented in Section 4.12, and the subsequent change in the model is presented in Section 4.13.

3.6.1.3. Linearity

The relationship of the independent and dependent variables should be linear, as further factor analysis is based on correlation (Pallant, 2009). To confirm linearity, a visual inspection of the scatterplots was done, there is no obvious indication of non-linearity in these graphs, our assumption of linearity is met (Tabachnick et al., 2013). Field (2013) also suggests that if a model is non-linear, the generalisation of the results is inhibited.

3.7. Quality Assurance

3.7.1. Reliability

According to Schindler (2019), reliability refers to the degree in which the research instrument produces data that free from random errors, and is consistent in providing data.

A Cronbach alpha score above 0.7 is regarded as having acceptable internal reliability (DeVellis & Thorpe, 2021). Although the commonly recognized value of 0.8 is adequate for cognitive assessments, Pallant (2020) observes that a cut-off point of 0.7 is better suitable for ability testing. According to Tavakol and Dennick (2011) explanation of the numerical output, which is assessed between 1 which denotes perfect internal reliability and 0 which indicates no internal reliability. Cronbach (1951) stated that the formula should be applied independently to items relevant to each factor if there are many factors, therefore in this study, to assess the data's internal reliability and confirm that the components are consistently and accurately recorded.

The reliability analysis was initially done on all theoretical constructs, and Table 2 indicates the SPSS internal reliability analysis. The overall scale indicates excellent reliability as the Cronbach alpha value (.962) exceeds the α=.700 score recommended by DeVellis and Thorpe (2021). All other sub-scale constructs "*Self-Efficacy*" (α = .913), "*Attitude"* (α = .967), "*Perceived Vulnerability"* (α = .920), "*Perceived Severity"* (α = .900), "*Subjective Norms"* (α = .920), "*Response Efficacy"* (α = .960) and "Cybersecurity Compliant behaviour*"* (α = .884), showed a high degree of reliability (> .7), suggesting that the item within each construct signifies the accuracy, stability, and predictability of the data collection instrument.

The detailed results of both the theoretical and empirical constructs are discussed in Section 4.11, where all Cronbach alpha values exceed .8 for the theoretical and empirical constructs.

Table 2: Cronbach Alpha on Theoretical constructs

Construct	Code	α Before Adjustment	No. of items	Items Deleted	α After Adjustment
Subjective Norms & Response Efficacy	SNRE	.951	8	-	.951
Attitude & Perceived Vulnerability	ATTPV	.961	9	-	.961
Self-Efficacy	SE	.913	4	-	.920
Perceived Severity	PS	.900	3	-	.900
Cybersecurity Compliant Behavior	CCB	.884	5	-	.884
Overall Scale *(All independent Items)*		.962	24	-	.962

3.7.2. Validity

Internal validity is fundamental for establishing research quality , and denotes the level of assurance that the causal relationship under test is reliable and unaffected by other variables (Schindler, 2019). In quantitative research, there are three different types of validity: construct validity, concurrent and predictive validity, and face and content validity, and this contributes to the instrument's ability to consistently deliver accurate measurements (Kumar, 2019).

In their study exploring the influences of individual decision styles on cybersecurity compliance ,Donalds and Osei-Bryson (2020) used exploratory factor analysis to establish validity. The systematic method followed, and the aim of their study was to establish which factors influence cybersecurity compliant behaviour.

The measurements will be grounded on a composition of established theories (Protection Motivation Theory and the Theory of Planned Behaviour), used widely in previous studies (Ajzen, 1985; Rogers, 1975). In order to measure the impact of the independent variables (Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-efficacy, Attitude, Subjective Norms) on cybersecurity compliant behaviour within a work-from home context, well-established theories and scales were adapted from previous studies (Hanus & Yu, 2016; Ifinedo, 2012; Li et al., 2019; Safa et al., 2015).

Furthermore, the instrument was initially piloted in January 2023, with a few peers in order to establish face validity, which allowed for further instrument refinement. This ensured that the questionnaire structure and questions were unambiguous and clearly identified.

3.8. Statistical Techniques

3.8.1. Exploratory Factor Analysis (EFA)

Exploratory Factor Analysis is the systematic simplification of linked metrics. EFA has historically been used to investigate potential underlying factor structures of a collection of observable variables without imposing a predetermined structure on the result (Child, 2006). In this research, the conceptual framework consisted of 6 independent variables, and therefore EFA provides a method to possibly produce a reduced number of linear combinations (Pallant, 2020).

Watkins (2018) presented a paper on the best practices for EFA, and as a multivariate statistical approach it has become an important instrument in the creation and validation of psychological theories and assessments. Furthermore, Hanus and Yu (2016) conducted an exploratory factor analysis to determine the underlying factors that inform Security Awareness towards desktop security behaviour with positive result. Similarly, James et al. (2013) used a five point Likert scale to explore the antecedents of digital security practices in the public domain while utilising an exploratory factor analysis to refine the research instrument and model by modification and removal of a number of questions in their original survey.

EFA was an applicable factor analysis, due to the research utilising a fairly new research instrument and model. While this was based on previously studies (Appendix A – Table 47) involving office work or the general population, there is almost no cybersecurity behavioural studies based on remote work. Therefore, EFA is used to explore the factor structure in order to confirm the final model and instrument. The process has been discussed further in Chapter 4, which commenced with an inter-item correlation matrix, utilizing a suitable factor extraction method, followed by a selection of a suitable 1st order and 2nd order rotation and retention methods (Pallant & Manual, 2007).

3.8.1.1. Inter Item Correlation

In this research, the significance of a correlation matrix was to display the relationship of the items measuring the same factor and those assessing distinct variables (Pallant, 2009). It provides information on which items measure the same underlying variable so that they may be grouped together. The expectation is for variables in one group to correlate more strongly than variables in other groups, achieving convergence and divergence validity (Tabachnick et al., 2013). The correlation value ranges between "0"and "1", and the closer to "1" the higher the correlation (Pallant, 2020). To ensure the factorability of the correlation matrix, should show many correlations coefficients of .3 or greater. Bartlett's test of sphericity should be statistically significant at $p < .005$ and the Kaiser-Meyer-Olkin value should be .6 or above. (Field, 2013).

3.8.1.2. Extraction of Factors.

The process of selecting the minimal number of factors that may be utilized to effectively depict the interrelationships among the collection of variables is known as factor extraction (Pallant, 2009). Principal axis factoring (PAF) with Kaiser's criterion and scree plot was the extraction technique used, as this extraction method does not make any distributional assumptions and is commonly used for Likert scale data that are not normally distributed, and is not symmetrical around the mean (Conway & Huffcutt, 2003). Therefore, according to Treiblmaier and Filzmoser (2010) no tests for normality have been done, as no specific distribution is required and it is not a prerequisite for Principal Axis Factoring. According to Field (2013) Kaiser's criterion was evaluated for all eigen values larger than one for the retention of applicable factors.

3.8.1.3. Factor Rotation

Factor rotation presents the pattern of loadings in a manner that is easier to interpret (Pallant, 2009). For the first order factor analysis, the Varimax rotation method was used, as it provides a simplified factor structure and distinctive factors (Field, 2013), and attempts to minimise the number of variables that have high loadings on each factor (Pallant, 2020). For the second order factor analysis, the extraction method was direct oblimin rotation, which is the most commonly used oblique technique and allows the

factors to correlate (Field, 2013; Pallant, 2020). According to Tabachnick et al. (2013) , at minimum, it is useful to try one oblique rotation method (direct oblimin), while examining the factor correlation matrix for values over ±0.32, and one orthogonal rotation method (Varimax).

3.8.2. Multiple Regression Analysis

Multiple regression analysis was used to investigate the relationship between a dependent variable and many independent factors, which allowed an understanding of how changes in the independent variables affect changes in the dependent variable while adjusting for the impact of other factors (Field, 2013). In a study by Ng et al. (2009) that investigated computer security behaviour of users, multiple regression was the recommended approach for testing the interactions of variables, to establish the outcomes of the hypotheses.

3.9. Ethical considerations

Schindler (2019) refers to ethics in the research process as the responsibility of ensuring safety, consent, anonymity and confidentiality of participants. In addition, maintaining an ethical posture regarding data reporting, how missing data is handled is also critical to establish credible conclusions for readers. (Creswell & Guetterman, 2018).

The study was conducted with the utmost regard for ethical considerations from the research proposal stage. Data collection only commenced after the ethical clearance was received from the University of Witwatersrand Ethics committee.

For this study, an informed consent form detailing the purpose of the study, time required for completion, and the data collection handling was included in the questionnaire. Respondents were notified of their anonymity and only demographic information pertinent to the study will be collected (Province, Education level and Business Sector). Furthermore, the online request requested participation consent as part of a mandatory question, indicated that participation was voluntary and requested approval for the data to be used for academic research only.

A copy of the cover letter illustrating the study objectives, detailed information and the informed consent inserted as part of question one in the research instrument is attached in Appendix A

4. PRESENTATION OF RESEARCH RESULTS

The main objective of this research study was to understand the factors influencing positive cybersecurity behaviour in a work-from-home environment. Firstly, for each factor, descriptive statistics show the measurements of central tendencies and dispersion. Secondly, a summary of participant responses to each concept is provided as part of the empirical research findings. This is followed by employing factor extraction methods to select the minimal number of factors that may be utilized to effectively depict the interrelationships among the collection of variables. In this research, the conceptual framework consisted of 6 independent variables, and therefore EFA provides a method to possibly produce a reduced number of linear combinations. Finally, multiple regression analysis was utilized to investigate the relationship between a dependent variable and independent factors, which allowed an understanding of how changes in the independent variables affect changes in the dependent variable while adjusting for the impact of other factors. An exploratory factor analysis was conducted to explore the factor structure based on the data collected. Regression analysis was used to test each hypothesis with the findings of related research questions are provided.

4.1. Description of Research respondents

The key demographic characteristics used to describe the respondents are location, education, and the industry. It was also important to gather the current status of the working environment in order to provide accurate information of the work from home status.

4.1.1. Work from home

Figure 4 illustrates the total responses of 188, of which 56 were excluded as they did not meet the work-from-home criteria. Therefore, those that were not afforded the opportunity to work from home during lockdown were removed from the dataset. Furthermore, the online questionnaire included a mechanism to bypass all subsequently questions to avoid gathering irrelevant data. After screening and cleaning of the data set, the sample size of 132 was used for further analysis. In addition, after the lockdown,

76.5% (*f* = 101) of the respondents are still working from home or spend some time during a work week at home.

Figure 4: Work from Home

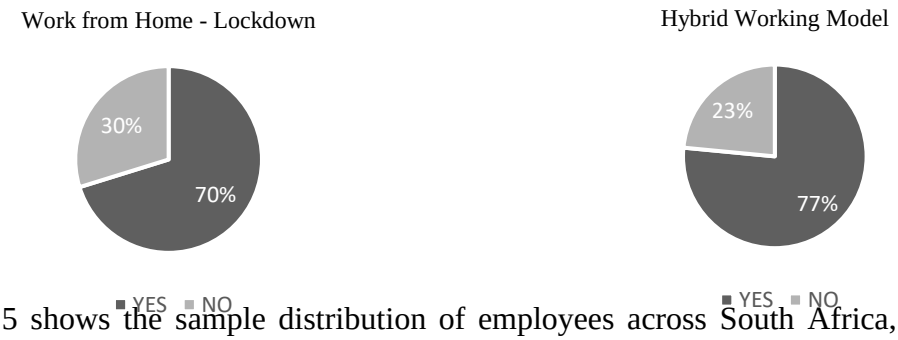
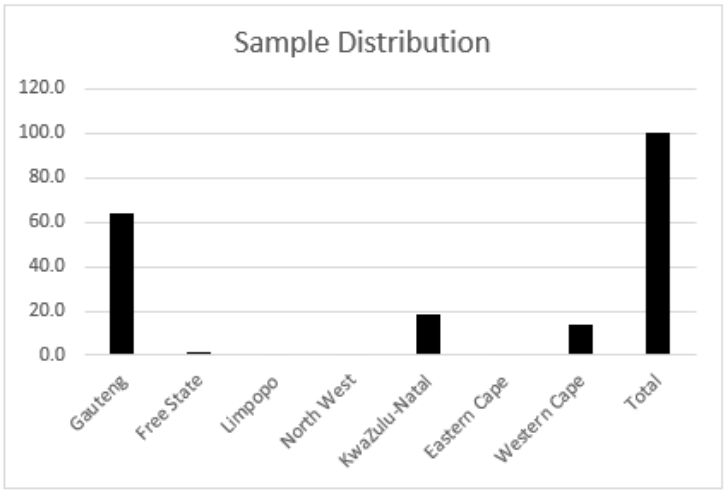


Figure 5 shows the sample distribution of employees across South Africa, and while respondents spanned across the seven provinces, the scatter was more predominant in Gauteng (64%), KZN (18%) and Western Cape (14%).

Figure 5: Sample Distribution



Gauteng	Free State	Limpopo	North West	KwaZulu-Natal	Eastern Cape	Western Cape	Total
64%	2%	1%	1%	18%	1%	14%	100%

Table 3 provides an illustration of the respondents' demographic data. The distribution in the final coded and cleaned sample of 132 respondents indicated a large percentage of respondents were based in Gauteng (31%, *f*=85) and KwaZulu-Natal (18%, *f*=24), followed by the Western Cape (13.6%, *f*=18)

The sample population included individuals with academic qualifications, the highest proportion of respondents, 50% (*f*=66) had obtained a bachelor's or honours degree, and

the second-highest portion of respondents, 31% (f=41) had obtained a certificate or diploma.

Finally, the demographic data captured the industry of respondents, with the telecommunications industry providing 57% (f=57) of the data. Second was IT (Information technology) (16%, f=22) and a similarly in the Banking and Financial (16%, f=22) industry. The total sample data was predominantly within the technology sector.

Table 3: Frequencies of Measures for Demographic

Demographics		*f*	%	Cumulative %
Province	Gauteng	85	64.4	64.4
	Free State	2	1.5	65.9
	Limpopo	1	0.8	66.7
	North West	1	0.8	67.4
	KwaZulu-Natal	24	18.2	85.6
	Eastern Cape	1	0.8	86.4
	Western Cape	18	13.6	100.0
Education	Primary/Secondary School	10	7.6	7.6
	Certificate/Diploma	41	31.1	38.6
	Bachelors/Honours Degree	66	50.0	88.6
	Master's Degree	15	11.4	100.0
Industry	Banking & Financial	21	15.9	15.9
	Education & Research	2	1.5	17.4
	Electrical Power & Energy Systems	2	1.5	18.9
	Health	3	2.3	21.2
	IT (Information Technology)	22	16.7	37.9
	Public Sector	6	4.5	42.4
	Transport	2	1.5	43.9
	Security (cyber)	1	0.8	44.7
	Telecommunications	57	43.2	87.9
	Other	16	12.1	100.0
Work from Home	Yes	101	76.5	76.5
	No	31	23.5	100.0

(N=132)

4.2. Descriptive Statistics Analysis

This section provides a summary of the descriptive statistics, indicating the measures and distribution of the key factors created.

Table 4 captures the factors that influence correct cybersecurity behaviour while in a work-from-home setting. The *"Self-efficacy"* construct provided an insight into employee's introspective ability to adhere to cybersecurity compliancy. The results were positive and exhibited a mean score of between 4.19 and 4.30 and a standard deviation (SD) of between 1.032 and 1.092.

The *"Attitude"* construct established the sentiment towards cybersecurity, resulting in a mean score between 4.45 and 4.67, and a standard deviation between 0.931 and 1.021. *"Perceived vulnerability"* indicated employees' sentiment towards a cyber threat and yielded a mean score between 4.57 and 4.64 with a standard deviation between 0.892 and 0.951. Item "ATT_Q12" had the highest overall mean and was meant to assess employees' information security awareness while working from home. More respondents agreed with the notion.

Table 4: Key Factors that Influence Cybersecurity behaviour.

Constructs	Items	N	Mean	Median	Min	Max	Std. Dev
Self-Efficacy	SE_Q7	132	4.24	5.00	1	5	1.092
	SE_Q8	132	4.28	5.00	1	5	1.036
	SE_Q9	132	4.30	5.00	1	5	1.062
	SE_Q10	132	4.19	5.00	1	5	1.085
Attitude	ATT_Q11	132	4.67	5.00	1	5	0.953
	ATT_Q12	132	4.66	5.00	1	5	0.931
	ATT_Q13	132	4.65	5.00	1	5	0.949
	ATT_Q14	132	4.45	5.00	1	5	1.021
	ATT_Q15	130	4.65	5.00	1	5	0.994
Perceived vulnerability	PV_Q16	132	4.57	5.00	1	5	0.951
	PV_Q17	132	4.55	5.00	1	5	0.935
	PV_Q18	132	4.64	5.00	1	5	0.909
	PV_Q19	132	4.64	5.00	1	5	0.892
Perceived severity	PS_Q20	132	4.53	5.00	1	5	1.015
	PS_Q21	132	4.52	5.00	1	5	1.122
	PS_Q22	131	4.50	5.00	1	5	1.112
Subjective Norms	SN_Q23	131	4.66	5.00	1	5	0.839
	SN_Q24	131	4.50	5.00	1	5	0.964
	SN_Q25	132	4.58	5.00	1	5	0.883
	SN_Q26	132	4.40	5.00	1	5	0.964
Response efficacy	RE_Q27	132	4.58	5.00	1	5	0.857
	RE_Q28	132	4.60	5.00	1	5	0.799
	RE_Q29	131	4.53	5.00	1	5	0.816
	RE_Q30	132	4.53	5.00	1	5	0.903
Cybersecurity compliant behavior	CCB_Q31	132	4.48	5.00	1	5	0.895
	CCB_Q32	132	4.54	5.00	1	5	0.842
	CCB_Q33	131	3.95	4.00	1	5	1.149
	CCB_Q34	132	4.42	5.00	1	5	0.883
	CCB_Q35	131	4.46	5.00	1	5	0.825

The "*Perceived severity"* construct capture employees view towards the potential of a cyberattack while working remotely. The resulting mean for the items range between 4.50 and 4.53 with a standard deviation between 1.015 and 1.122. All items were centred around "agree", and most respondents believe that a data breach could cause extensive damage to company data assets.

The construct *"Subjective norms"* is a behavioural predictor and alludes to the notion that normative views are established because of social pressure, and yielded a mean between 4.40 and 4.66, and a standard deviation between 0.839 and 0.964. Most respondents agreed with item "SN_Q23" within this construct, with the highest mean of 4.66, which ascertains that they believe that managerial pressure to follow cyber security policies was regarded as the most influential.

The benefits of the person's actions as perceived by them are described by the construct *"Response efficacy"*. The results indicated a mean range between 4.53 and 4.60, and a and a standard deviation between 0.799 and 0.903. Employees installing antivirus software is indicated by the item "RE_Q27,", whilst item "RE_Q28" revealed monitoring regular antivirus updates. Both items showed the highest means within this scale.

Lastly, the "*Cybersecurity Compliant Behaviour*" construct represented the measures adopted by the employee to further enhance information security. The results indicated a mean score between 3.95 and 4.48 and a standard deviation between 0.825 and 1.149. While all items centred around agree, the lowest overall mean was item "CCB_Q33", which indicated consultation with security experts while working from home.

4.3. Self-Efficacy

4.3.1. Presentation of the Empirical Results

This section provides a summary of the empirical findings that were obtained through the use of descriptive statistics to determine the relationship between employee's self - efficacy and their intentions to adhere to correct cyber security compliant behaviour.

Table 5 presents the descriptive statistical analysis in relation to the "*Self-efficacy*" construct. These items were utilised within the questionnaire to understand an employee's self-confidence in possessing the skills to defend against cyber security attacks.

There were four items within the "*Self-efficacy*" construct. "SE_Q7", "SE_Q8" and "SE_Q9" indicated the perception of the employee's current skills and expertise to deal with information security violations while working from home. "SE_Q10" illustrated the overall control felt by employees in a remote working context.

Table 5: Descriptive Statistics - Self-efficacy

Item		Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Total
SE_Q7	Count	7	6	6	42	71	132
	Row N %	5.3%	4.5%	4.5%	31.8%	53.8%	100.0%
SE_Q8	Count	5	7	6	42	72	132
	Row N %	3.8%	5.3%	4.5%	31.8%	54.5%	100.0%
SE_Q9	Count	5	9	3	39	76	132
	Row N %	3.8%	6.8%	2.3%	29.5%	57.6%	100.0%
SE_Q10	Count	5	9	10	40	68	132
	Row N %	3.8%	6.8%	7.6%	30.3%	51.5%	100.0%

The results indicated that 31.8% (Somewhat Agreed) and 53.8% (Strongly agreed) respectively, to having the expertise to implement preventative measures to migrate cyber threats, which accounts for more than 86% of all respondents. Furthermore, only 10% of respondents felt that that are unequipped to handle cyber threats, while only 4.7% were neutral (Neither agree nor disagree) in responses.

4.4. Attitude towards Cyber Security

4.4.1. Presentation of the Empirical Results

This section presents an overview of the empirical results, to illustrate employee's attitude towards cyber security while in a remote working context. This construct utilized five items to understand employee's attitude towards cybersecurity while working from home.

Table 6 illustrates employee's attitude towards information security regarding cyber threats. All items show considerable positivity towards cybersecurity. "ATT_Q11", "ATT_Q12" and "ATT_Q13" indicated a majority of above 92.4% Agreed or Strongly

Agreed that information security is necessary, beneficial, and useful while working from home.

Furthermore, item "ATT_Q14" shows that 88.7% of respondents had a positive outlook on information security. From the total sample size of 132 respondents, (63.68%) Agreed (11.1%) and Strongly Agreed (80.7%), whilst 6% either Disagreed or Strongly Disagreed.

Table 6: Descriptive Statistics - Attitude towards Cybersecurity

Item		Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Total
ATT_Q11	Count	6	3	0	10	113	132
	Row N %	4.5%	2.3%	0.0%	7.6%	85.6%	100.0%
ATT_Q12	Count	5	4	0	13	110	132
	Row N %	3.8%	3.0%	0.0%	9.8%	83.3%	100.0%
ATT_Q13	Count	6	2	2	12	110	132
	Row N %	4.5%	1.5%	1.5%	9.1%	83.3%	100.0%
ATT_Q14	Count	5	6	4	27	90	132
	Row N %	3.8%	4.5%	3.0%	20.5%	68.2%	100.0%
ATT_Q15	Count	8	0	1	11	110	130
	Row N %	6.2%	0.0%	0.8%	8.5%	84.6%	100.0%

4.5. Perceived Vulnerability

This section provides a summary of the empirical findings that were obtained through the use of descriptive statistics to access an employee's perceived vulnerability whilst in a remote working environment.

4.5.1. Presentation of the Empirical Results

Descriptive statistical analysis relating to the "Perceived Vulnerability" construct is presented in Tables 7. The fours items were used to determine the perception of vulnerability felt by employees and the resulting negative effects on company assets due to non-adherence of cyber security compliant behaviour.

In Table 7, "PV_Q16" indicated the vulnerability to security breaches if company mandated security policies and procedures where not followed while working from home. The results show a majority of 90.1% either agreed or strongly agreed to following company policies in order to safeguard information assets. Furthermore "PV_Q17"

focused on vulnerability to malicious attacks, and comparably 90.2% agreed that it is imperative to follow organisational guidelines to cybersecurity compliance.

Table 7: Descriptive Statistics - Perceived Vulnerability

Item		Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Total
PV_Q16	Count	4	5	4	18	101	132
	Row N %	3.0%	3.8%	3.0%	13.6%	76.5%	100.0%
PV_Q17	Count	2	9	2	20	99	132
	Row N %	1.5%	6.8%	1.5%	15.2%	75.0%	100.0%
PV_Q18	Count	4	4	3	13	108	132
	Row N %	3.0%	3.0%	2.3%	9.8%	81.8%	100.0%
PV_Q19	Count	5	1	4	16	106	132
	Row N %	3.8%	0.8%	3.0%	12.1%	80.3%	100.0%

4.6. Perceived Severity

This section provides a summary of the empirical findings that were obtained through the use of descriptive statistics to assess an employee's perceived severity whilst in a remote working environment.

4.6.1. Presentation of the Empirical Results

While perceived vulnerability is the magnitude of the consequences when the negative outcome occurs, perceived severity refers to the likelihood of a negative event. Therefore, the three items depicted in Table 8, was utilized to acquire employee's perception on the severity of a breach via their computer device at home.

The results for all three scale items were primarily centred on "Agree" that contributed to the largest overall percentage The average response within the "*Perceived Severity*" sub-scale can be described as Disagreed (8.4%), Agreed (88.4%) and Neutral (3.3%).
"PS_Q22" meant to capture an employee's severity rating on losing organisation's data from hacking rated highly at 88.1%.

Table 8: Descriptive Statistics - Perceived Severity

Item		Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Total
PS_Q20	Count	7	1	6	19	99	132
	Row N %	5.3%	0.8%	4.5%	14.4%	75.0%	100.0%
PS_Q21	Count	9	3	3	12	105	132
	Row N %	6.8%	2.3%	2.3%	9.1%	79.5%	100.0%
PS_Q22	Count	7	6	4	12	102	131
	Row N %	5.3%	4.6%	3.1%	9.2%	77.9%	100.0%

4.7. Subjective Norms

This section presents an overview of the empirical results, to illustrate how the influence of people in their social and work environment influence their particular conduct towards cyber security while in a remote working context.

4.7.1. Presentation of the Empirical Results

Subjective norms are a behavioural predictor and refers to the idea that prescriptive views are those formed as a result of social pressure from those in your immediate circle. To assess the influence in a cybersecurity context, the four items below were used to gather information regarding an employee's normative views.

Table 9 depicts the descriptive analysis of the items across the spectrum of responses. "SN_Q23" explored the external pressures of employee's managers to adhere to cybersecurity compliant behaviour. With the highest positive responses of all items, respondents strongly agree (80.9%) and somewhat agreed (9.9%) to managerial influence. However, for all four items in the scale, the results most centred around direct influence from co-workers, IT staff and subordinates. (86.9%, agree and strongly agree), whilst 8.4% remained neutral.

Table 9: Descriptive Statistics - Subjective norms

Item		Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Total
SN_Q23	Count	3	2	7	13	106	131
	Row N %	2.3%	1.5%	5.3%	9.9%	80.9%	100.0%
SN_Q24	Count	3	5	11	17	95	131
	Row N %	2.3%	3.8%	8.4%	13.0%	72.5%	100.0%
SN_Q25	Count	3	3	8	18	100	132
	Row N %	2.3%	2.3%	6.1%	13.6%	75.8%	100.0%
SN_Q26	Count	3	3	18	22	86	132
	Row N %	2.3%	2.3%	13.6%	16.7%	65.2%	100.0%

4.8. Response efficacy towards Cyber Security

This section presents an overview of the empirical results, using descriptive statistics, to illustrate employee's response towards cyber security while in a remote working environment.

4.8.1. Presentation of the Empirical Results

Response efficacy is viewed as a unique personality attribute that can be effectively used to correlate behavioural intents and certain cybersecurity behaviours. Therefore, the four items in this subscale were used to understand the steps that employees will undertake to pre-empt any security threats, to mitigate data breaches.

Table 10 illustrates the four items that contribute to correct cyber security behaviour. "RE_Q27" is a depiction of employees installing antivirus software and subsequently "RE_Q28" focused on frequent antivirus updates. Both items centred around a positive outlook with an average of 93.9% that agreed.

Table 10: Descriptive Statistics - Response Efficacy

Item		Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Total
RE_Q27	Count	4	2	2	30	94	132
	Row N %	3.0%	1.5%	1.5%	22.7%	71.2%	100.0%
RE_Q28	Count	2	4	2	29	95	132
	Row N %	1.5%	3.0%	1.5%	22.0%	72.0%	100.0%
RE_Q29	Count	2	3	6	32	88	131
	Row N %	1.5%	2.3%	4.6%	24.4%	67.2%	100.0%
RE_Q30	Count	4	2	7	26	93	132
	Row N %	3.0%	1.5%	5.3%	19.7%	70.5%	100.0%

4.9. Dependant Variable: Cybersecurity compliant behaviour

This section presents an overview of the empirical results of "*Cybersecurity compliant behaviour*", that was used against the independent variables (*Response Efficacy, Subjective Norms, Perceived Vulnerability, Attitude, Perceived Severity, Self-Efficacy*) to determine how these constructs influence correct cybersecurity behaviour.

4.9.1. Presentation of the Empirical Results

Item "CCB_Q31" was used to determine if employees consider security expert's recommendations while working remotely. The results indicated 125 respondents (67.4%) Agreed (19.7%) and Strongly Agreed (67.4%) to adherence to security guidelines. Furthermore, "CCB_Q33" is meant to capture the direct communication with security experts prior to any actions regarding information while working from home. The results in Table 11 indicate that 91 respondents consult IT experts while 23 (17.6%) remained neutral.

Table 11: Descriptive Statistics - Cybersecurity Compliant behaviour

Item		Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Total
CCB_Q31	Count	1	7	9	26	89	132
	Row N %	0.8%	5.3%	6.8%	19.7%	67.4%	100.0%
CCB_Q32	Count	1	6	6	27	92	132
	Row N %	0.8%	4.5%	4.5%	20.5%	69.7%	100.0%
CCB_Q33	Count	5	12	23	35	56	131
	Row N %	3.8%	9.2%	17.6%	26.7%	42.7%	100.0%
CCB_Q34	Count	1	5	14	30	82	132
	Row N %	0.8%	3.8%	10.6%	22.7%	62.1%	100.0%
CCB_Q35	Count	1	4	10	35	81	131
	Row N %	0.8%	3.1%	7.6%	26.7%	61.8%	100.0%

4.10. Exploratory Factor Analysis

The EFA results for each of the analysed constructs are reported and interpreted at the beginning of the chapter.

All of the item scales were subjected to exploratory factor analysis using SPSS V28 to ascertain the number and makeup of factors. As a way to essentially examine the link between factors and their observed variables, it was also used to assess the convergence and divergence of the various items and factors (Pallant, 2009). Principal axis factoring (PAF) with Kaiser's criterion and scree plot, was the extraction technique used, as this extraction method does not make any distributional assumptions and is commonly used for Likert scale data that are not normally distributed and is not symmetrical around the mean (Conway & Huffcutt, 2003). Therefore, according to Treiblmaier and Filzmoser

(2010) no tests for normality have been done, as no specific distribution is required and it is not a prerequisite for Principal axis factoring.

For the first order factor analysis, the Varimax rotation method was used, as it provides a simplified factor structure and distinctive factors (Field, 2013), and attempts to minimise the number of variables that have high loadings on each factor (Pallant, 2020). For the second order factor analysis, the extraction method was direct oblimin rotation, which is the most commonly used oblique technique and allows the factors to correlate (Field, 2013; Pallant, 2020). According to Tabachnick et al. (2013) , at minimum, it is useful to try one oblique rotation method (direct oblimin), while examining the factor correlation matrix for values over ±0.32, and one orthogonal rotation method (Varimax).

4.10.1. Cybersecurity Compliant Behaviour (Dependant Variable)

The scale evaluating *Cybersecurity Compliant Behaviour* was subjected to exploratory factor analysis. The inter-item correlation of the five four questions used to measure the dependant variable *Cybersecurity Compliant Behaviour* is shown in Table 12. The outcome indicates that every item correlates with its corresponding scale as all inter-item correlations are above 0.3 (Tabachnick et al., 2013). Therefore, no items were removed, and the scale show convergence validity.

Table 12: Inter Item Correlation Coefficients (Cybersecurity Compliant Behaviour)

	CCB_Q31	CCB_Q32	CCB_Q33	CCB_Q34	CCB_Q35
CCB_Q31	1.000				
CCB_Q32	.801	1.000			
CCB_Q33	.654	.555	1.000		
CCB_Q34	.565	.567	.463	1.000	
CCB_Q35	.733	.717	.557	.634	1.000

Bartlett's Test of Sphericity, presented in Table 13 was highly significant ($p < .005$) and the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy value of .855 supported the factorability of the matrix (Pallant, 2009). Furthermore, the Kaiser-Meyer-Olkin (KMO) measures sampling adequacy and the Bartlett test of Sphericity was used to verify if the data was suitable for factor analysis. According to Kumar (2019), a KMO score above .6 and a statistically significant Bartlett's Test of Sphericity indicates the adequacy of the sample to pass factor analysis. Therefore, the results in Table 13 show the KMO

value of .855, which indicates that the sample size and set of variables are adequate for further factor analysis.

Table 13: KMO and Bartlett's Test (Cybersecurity Compliant Behaviour).

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.855
Bartlett's Test of Sphericity	Approx. Chi-Square	386.884
	df	10
	Sig.	.000

In addition, the Anti-image Matrices and communalities were also evaluated (Appendix B Table 48). The measures of sampling adequacy test indicate all MSA values above .6, ranging from .803 to .902 which indicates no weak items that needs to be removed. The communalities at extraction yielded results within the range of .453 and .811 which is above .3 (Pallant, 2009, p. 190), and at least 40% common variance shared between the items.

4.10.1.1. Factor Extraction

Table 14 represented the Total Variance Explained, where only one Eigenvalue was above one, indicating that that this factor explains 70 % of the variance. The Factor matrix is also provided in Appendix B (Table 49) where all values are above > .05, and all five items loaded on a single factor. There was no rotation necessary as only a single factor was extracted.

Table 14: Total Variance Explained (Cybersecurity Compliant Behaviour).

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Varian	Cumulative %	Total	% of Variance	Cumulative %
1	**3.514**	70.275	**70.275**	3.176	63.517	63.517
2	.561	11.223	81.499			
3	.460	9.200	90.698			
4	.280	5.609	96.307			
5	.185	3.693	100.000			

Extraction Method: Principal Axis Factoring.

4.10.2. Independent Variables

The data sample was assessed for its suitability for factor analysis and the inter item correlation for each independent variable is presented in Section 4.11. Bartlett's Test of Sphericity was highly significant ($p < .005$) and the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy value of .918 supported the factorability of the correlation matrix (Pallant, 2009). Table 15 show the overall KMO value of .918, which indicates that the sample size and set of variables are adequate for further factor analysis. Based on Bartlett's test results of Approx. Chi-Square=3393.308 and p=0.00(<0.05), indicating statistical significance (Pallant & Manual, 2007), therefore supporting the factorability of the correlation matrix.

Table 15: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.918
Bartlett's Test of Sphericity	Approx. Chi-Square	3393.308
	df	276
	Sig.	0.000

The measures of sampling adequacy test indicate all MSA values above .6, ranging from .803 to .902 which indicates no weak items that needs to be removed. The communalities at extraction ranged between 0.579 and 0.876 which is greater than 0.3, which is at least 50% common variance shared between the items (Pallant, 2009). The full representation of the communalities is attached in Appendix B (Table 50).

In addition, the values for the anti-image correlation above .832 (>.6) so the sampling results exceed the required adequacy (Field, 2013; Pallant, 2020), therefore no items required omission. This is presented in Appendix B (Table 51)

4.10.2.1. Factor Extraction

Principal axis factoring analysis revealed the presence of four components with eigen values exceeding 1 according to the Kaiser's criterion (Pallant & Manual, 2007), with totals of 13.467, 2.328, 1.77 and 1.106 explaining 56%, 9.7%, 7.4% and 4.7% of the variance respectively. The results from Table 16 shows that the four empirical factors extracted explained a total variance of 77.8% before rotation and 73.7% after rotation.

A further inspection of the scree plot revealed a break after the fourth factors, and all subsequent factors are below the eigen value of 1.

Table 16: Total Variance Explained.

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	**13.476**	56.151	56.151	13.221	55.089	55.089	5.837	24.322	24.322
2	**2.328**	9.700	65.851	2.068	8.617	63.706	5.385	22.439	46.760
3	**1.770**	7.376	73.227	1.525	6.355	70.061	3.880	16.166	62.926
4	**1.106**	4.608	**77.835**	.872	3.632	73.693	2.584	10.767	**73.693**
5	.907	3.779	81.614						
6	.728	3.034	84.648						
7	.445	1.855	86.502						
8	.390	1.627	88.129						
9	.368	1.534	89.663						
10	.342	1.426	91.090						
11	.288	1.202	92.291						
12	.275	1.145	93.436						
13	.259	1.081	94.517						
14	.229	.955	95.472						
15	.203	.844	96.316						
16	.165	.688	97.004						
17	.144	.600	97.605						
18	.139	.577	98.182						
19	.109	.454	98.636						
20	.092	.382	99.018						
21	.083	.346	99.365						
22	.066	.273	99.638						
23	.056	.233	99.870						
24	.031	.130	100.000						

Extraction Method: Principal Axis Factoring.

Table 17 illustrates the rotated factor matrix, where each item has a loading on each of the four factors, however the highest loading has been grouped within a single factor. The theoretical model consisted of 6 independent variables (*Response Efficacy, Subjective Norms, Perceived Vulnerability, Attitude, Perceived Severity, Self-Efficacy*) however following results of the factor extraction, there was a grouping of items within the factors that have now resulted in four empirical factors. The results show the combination of items for the Subjective *Norms* and *Response Efficacy* construct of the PMT model, which was identified as Factor one in the rotated factor matrix. Furthermore, the construct *Attitude* which is part of the TPB model also combined with the *Perceived Vulnerability* from the PMT model, which yielded Factor two. The extraction of Factor three and four remained the same as the theoretical constructs of *Perceived Severity and Self-Efficacy* respectively.

Table 17: Rotated Factor Matrix.

	Factor			
	1	2	3	4
RE_Q27	**.723**	.394	.277	.133
RE_Q29	**.779**	.319	.245	.077
RE_Q28	**.773**	.340	.288	.105
RE_Q30	**.765**	.304	.250	.131
SN_Q23	**.761**	.215	.303	.322
SN_Q26	**.747**	.163	.213	.217
SN_Q24	**.709**	.228	.232	.213
SN_Q25	**.615**	.291	.207	.312
ATT_Q15	.246	**.766**	.417	.128
ATT_Q13	.246	**.741**	.394	.196
ATT_Q12	.285	**.727**	.436	.194
ATT_Q11	.266	**.720**	.485	.230
ATT_Q14	.294	**.595**	.467	.113
PV_Q17	.311	**.667**	.170	.229
PV_Q18	.417	**.738**	.209	.171
PV_Q19	.527	**.590**	.139	.225
PV_Q16	.360	**.554**	.071	.327
SE_Q8	.263	.229	**.811**	.024
SE_Q10	.267	.207	**.787**	.031
SE_Q9	.333	.264	**.734**	.065
SE_Q7	.188	.259	**.689**	.016
PS_Q22	.206	.155	.061	**.894**
PS_Q21	.218	.231	.024	**.824**
PS_Q20	.303	.467	.012	**.599**

Extraction Method: Principal Axis Factoring.
Rotation Method: Varimax with Kaiser Normalization.
Rotation converged in 7 iterations.

4.10.3. 2nd Order Factor Analysis

The identified four factors in the second order factor analysis was used for factorability. According to Tabachnick et al. (2013) , at minimum, it is useful to try one oblique rotation method (direct oblimin), while examining the factor correlation matrix for values over ±0.32. The inter-item correlation of the four constructs used to measure the dependant variable *Cybersecurity Compliant Behaviour* is shown in Table 18. The outcome indicates that correlations values all exceed .3 (Tabachnick et al., 2013).

Table 18: Correlation Matrix (Independent Factors)

	Subjective Norms & Response Efficacy	Attitude & Perceived Vulnerability	Self-Efficacy	Perceived Severity
Subjective Norms & Response Efficacy	1.000			
Attitude & Perceived Vulnerability	.773	1.000		
Self-Efficacy	.636	.681	1.000	
Perceived Severity	.569	.607	.292	1.000

Table 19 show the KMO value of .746, and the Bartletts test of Sphericity, the p-value of p=.000(<0.05), indicating statistical significance (Pallant & Manual, 2007), therefore supporting the factorability of the correlation matrix. Furthermore, the Measures of sampling adequacy indicate all MSA values above .6. The communalities at extraction were all greater than 0.3 and is attached to Appendix B (Table 50)

Table 19: KMO and Bartlett's Test (2nd order Factor Analysis).

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.746
Bartlett's Test of Sphericity	Approx. Chi-Square	278.891
	df	6
	Sig.	.000

Table 20 yielded one factor with eigen values exceeding 1 according to the Kaiser's criterion (Pallant & Manual, 2007), which explained that behavioural influence of cybersecurity perceptions. The total of 2.804 explained 70% of the variance.

Table 20: Total Variance Explained (2nd Order Factor Analysis).

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	**2.804**	70.101	**70.101**	2.485	62.127	62.127
2	0.711	17.768	87.868			
3	0.278	6.959	94.827			
4	0.207	5.173	100.000			

Extraction Method: Principal Axis Factoring.

Appendix B (Table 54) illustrates the results of the anti-image correlation where the matrix contains measures of sampling adequacy for each variable along the diagonal and the negatives of the partial correlation/covariances on the off-diagonals.

4.11. Theoretical, Empirical Reliabilities and Correlations

To assess the reliability of the questionnaire, a reliability analysis was performed. Cronbach's alpha reliability coefficient was used to assess the item's internal consistency.

In this research, a correlation matrix was important to highlight any relationships between items measuring the same variable and those assessing other dependant variables. It provides information on which items measure the same underlying variable so that they may be grouped together. The expectation is for the constructs in one group to correlate more strongly than constructs in other groups, achieving convergence and divergence validity (Tabachnick et al., 2013). The correlation value ranges between "0"and "1", and the closer to "1" the higher the correlation (Pallant, 2020). The reliability test was firstly conducted on all theoretical factors in the conceptual framework and based on the results of the exploratory factor analysis (EFA) in the previous Section 4.10., was thereafter conducted on the empirical factors.

4.11.1. Self-Efficacy

The reliability for the four items represents meant to capture Self-Efficacy in Table 21 show $\alpha = .913$ (> .7) before adjustment, which indicates good reliability. The deletion of "SE_Q7" would have adjusted the overall score by 0.001, however the result would not have produced significant improvement, therefore all items here retained.

Table 21: Item-Total Statistics (Self-Efficacy)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
SE_Q7	12.77	8.650	.728	.914	.913
SE_Q8	12.73	8.364	.848	.872	
SE_Q9	12.71	8.390	.812	.884	
SE_Q10	12.83	8.206	.826	.879	

The inter-item correlation matrix of the four questions used to measure *Self-Efficacy* is shown in Table 22. The outcome indicates that every item correlates with its corresponding scale as all inter-item correlations are above .651 (> .3). Therefore, no items were removed, and all scales show convergent validity.

Table 22: Inter Item Correlation (Self-Efficacy)

	SE_Q7	SE_Q8	SE_Q9	SE_Q10
SE_Q7	1.000			
SE_Q8	.704	1.000		
SE_Q9	.651	.767	1.000	
SE_Q10	.668	.785	.728	1.000

4.11.2. Attitude

The Scale reliability is presented in Table 23, where the total value is α = .967 (> .7). None of the items here would substantially improve reliability if they were removed, therefore all five items were preserved for further analysis.

Table 23: Item-Total Statistics (Attitude)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
ATT_Q11	18.41	13.375	.954	.951	
ATT_Q12	18.43	13.627	.935	.955	
ATT_Q13	18.43	13.627	.914	.958	.967
ATT_Q14	18.64	13.550	.843	.970	
ATT_Q15	18.43	13.503	.888	.962	

The five questions used to measure employees' attitude are presented in Table 24. The outcome demonstrates that all inter-item correlations are above .751 (> .3), demonstrating that all items correlate with the corresponding scales. Consequently, each scale has convergent validity.

Table 24: Inter Item Correlation (Attitude)

	ATT_Q11	ATT_Q12	ATT_Q13	ATT_Q14	ATT_Q15
ATT_Q11	1.000				
ATT_Q12	.947	1.000			
ATT_Q13	.890	.872	1.000		
ATT_Q14	.815	.802	.777	1.000	
ATT_Q15	.868	.833	.845	.751	1.000

4.11.3. Perceived Vulnerability

Table 25 presents the overall reliability of the scale. The value for alpha (α = .920) could not be improved with the deletion of any of the four items, as the result already reflected a good degree of reliability.

Table 25: Item-Total Statistics (Perceived Vulnerability)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
PV_Q16	13.84	6.394	.765	.914	.920
PV_Q17	13.86	6.139	.855	.884	
PV_Q18	13.77	6.303	.843	.885	
PV_Q19	13.77	6.517	.804	.886	

The inter-item correlation of the four questions used to measure *Perceived Vulnerability* is shown in Table 26. The outcome indicates that every item correlates with its corresponding scale as all inter-item correlations are above .624 (> .3). Therefore, no items were removed, and all scales show convergence validity.

Table 26: Inter Item Correlation (Perceived Vulnerability)

	PV_Q16	PV_Q17	PV_Q18	PV_Q19
PV_Q16	1.000			
PV_Q17	.743	1.000		
PV_Q18	.624	.796	1.000	
PV_Q19	.643	.683	.778	1.000

4.11.4. Perceived Severity

The reliability for the three items in Table 27 show an α=0.900 (> .7) before adjustment, which indicates a good degree of reliability. The overall value would have increased if " PS_Q20" had been deleted, however it was retained to preserve the minimum requirement of three items per construct. A similar study by Li et al. (2019) investigated the employee's cybersecurity behaviour, produced an alpha value (α = .840) for the original scale, thus re-establishing the internal consistency of the scale.

Table 27: Item-Total Statistics (Perceived Severity)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
PS_Q20	9.02	4.677	.713	.929	.900
PS_Q21	9.02	3.838	.850	.816	
PS_Q22	9.05	3.875	.854	.811	

The three questions used to measure employees *Perceived Severity* are presented in Table 28. The outcome demonstrates that all inter-item correlations are above .661 (> .3), demonstrating that all items correlate with the corresponding scales. Consequently, each scale has convergent validity.

Table 28: Inter Item Correlation (Perceived Severity)

	PS_Q20	PS_Q21	PS_Q22
PS_Q20	1.000		
PS_Q21	.660	1.000	
PS_Q22	.666	.857	1.000

4.11.5. Subjective Norms

Table 29 consists of four relatively new items to measure the subjective norms during work from home environments. The scale showed a good internal consistency, with a Cronbach alpha coefficient value where α = .920. All items were retained as per the original scale, as the removal of "SN_Q25" would have seen a minimal difference to the overall alpha result.

Table 29: Item-Total Statistics (Subjective Norms)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
SN_Q23	13.54	5.863	.895	.870	.920
SN_Q24	13.67	5.820	.804	.890	
SN_Q25	13.60	6.226	.735	.922	
SN_Q26	13.77	5.698	.833	.889	

The inter-item correlation of the four questions used to measure *Subjective Norms* is shown in Table 30. The outcome indicates that every item correlates with its

corresponding scale as all inter-item correlations are above .632 (> .3). Therefore, no items were removed, and all scales show convergence validity.

Table 30: Inter Item Correlation (Subjective Norms)

	SN_Q23	SN_Q24	SN_Q25	SN_Q26
SN_Q23	1.000			
SN_Q24	.829	1.000		
SN_Q25	.777	.632	1.000	
SN_Q26	.799	.778	.695	1.000

4.11.6. Response Efficacy

The reliability for the four items in Table 31 show α = .960 (> .7) before adjustment, which indicates a good degree of reliability. The value for alpha could not be improved with the deletion of any of the four items, as the result already reflected a good degree of reliability.

Table 31: Item-Total Statistics (Response-Efficacy)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
RE_Q27	13.66	5.796	.899	.949	.960
RE_Q28	13.63	5.957	.934	.940	
RE_Q29	13.69	5.968	.908	.946	
RE_Q30	13.70	5.657	.877	.957	

The four items used to measure employees *Response Efficacy* are presented in Table 32. The outcome demonstrates that all inter-item correlations are above .781 (> .3), demonstrating that all items correlate with the corresponding scales. Consequently, each scale has convergent validity.

Table 32: Inter Item Correlation (Response Efficacy)

	RE_Q27	RE_Q28	RE_Q29	RE_Q30
RE_Q27	1.000			
RE_Q28	.918	1.000		
RE_Q29	.821	.854	1.000	
RE_Q30	.781	.828	.868	1.000

4.11.7. Cyber security compliant behaviour (Dependent Variable)

A reliability evaluation shown in Table 33 for the dependent variable consisting of five items. The scale showed a good internal consistency, with a Cronbach alpha coefficient value of α = .884 (> .7). All items were retained for further analysis, as any removal showed no significant gain in the total alpha value.

Table 33: Item-Total Statistics (Cyber security compliant behaviour)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
CCB_Q31	17.34	9.373	.829	.834	.884
CCB_Q32	17.28	9.876	.781	.847	
CCB_Q33	17.35	9.982	.781	.848	
CCB_Q34	17.86	8.988	.643	.889	
CCB_Q35	17.40	10.335	.636	.878	

4.11.8. Subjective Norms & Response Efficacy (Empirical)

The new empirical factor which resulted in the combination of the two theoretical distinct factors (*Subjective Norms & Response Efficacy)* was subjected to further reliability testing to ensure that all combined items still meet the reliability criteria. The new factor has good internal consistency, with a Cronbach alpha coefficient reported of α = .951 as indicated in Table 34. Therefore, no items were removed, and the new scale was considered as reliable.

Table 34: Subjective Norms & Response Efficacy (Empirical)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
RE_Q29	31.95	26.654	.846	.943	.951
RE_Q28	31.89	26.707	.862	.942	
RE_Q30	31.95	25.888	.831	.943	
SN_Q23	31.86	25.637	.878	.940	
SN_Q26	32.09	25.507	.803	.945	
RE_Q27	31.91	26.297	.837	.943	
SN_Q24	31.99	25.680	.787	.946	
SN_Q25	31.92	26.494	.727	.950	

4.11.9. Attitude & Perceived Vulnerability (Empirical)

As a result of the EFA, the combination of the two distinct theoretically factors *(Attitude and Perceived Vulnerability*), which was then subjected to additional reliability testing to ensure that all merged items continue to fulfil the reliability requirements. Table 35 indicates that the new factor has strong internal consistency, with a reported Cronbach alpha coefficient of α = .961. No items were eliminated, so the new scale was deemed to be reliable.

Table 35: Attitude & Perceived Vulnerability (Empirical)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Alpha
ATT_Q15	36.83	43.444	.892	.953	
ATT_Q14	37.04	44.177	.797	.958	
ATT_Q13	36.83	44.033	.882	.954	
ATT_Q12	36.83	44.033	.900	.953	
ATT_Q11	36.81	43.660	.911	.952	.961
PV_Q19	36.84	45.780	.785	.958	
PV_Q18	36.85	44.612	.872	.954	
PV_Q17	36.93	45.150	.797	.958	
PV_Q16	36.92	46.087	.702	.962	

4.12. Summary of Reliability

The reliability analysis was initially done on all theoretical constructs, where Table 36 indicates the SPSS internal reliability analysis. The overall scale indicates excellent reliability as the Cronbach alpha value (.962) exceeds the α=.7 score recommended by DeVellis and Thorpe (2021). All other sub-scale constructs "*Self-Efficacy*", (α = .913), "*Attitude"* (α = .967), "*Perceived Vulnerability"* (α = .920), "*Perceived Severity"* (α = .900), "*Subjective Norms"* (α = .920), "*Response Efficacy"* (α = .960) and "*Cybersecurity Compliant Behaviour".* (α = .884), showed a high degree of reliability (> .7), suggesting that the item within each construct signifies the accuracy, stability, and predictability of the data collection instrument.

Table 36: Cronbach Alpha for Internal Reliability (Theoretical)

Construct	Code	α Before Adjustment	No. of items	Items Deleted	α After Adjustment
Self-Efficacy	SE	.913	4	-	.913
Attitude	ATT	.967	5	-	.967
Perceived Vulnerability	PV	.920	4	-	.920
Perceived Severity	PS	.900	3	-	.900
Subjective Norms	SN	.920	4	-	.920
Response Efficacy	RE	.960	4	-	.960
Cybersecurity Compliant Behavior	CCB	.884	5	-	.884
Overall Scale *(All independent Items)*		.962	24	-	.962

A reliability study was thereafter performed on all empirical constructs following the EFA results, to confirm that the new factors still adhere to the reliability standards. Table 37 indicates the three factors that are also part of the theoretical framework (*Perceived Severity, Subjective Norms and Cybersecurity Compliant behaviour*), and the two new constructs. Both empirical constructs "*Subjective Norms & Response Efficacy*" (α = .951), and "*Attitude & Perceived Vulnerability"* (α = .961), still maintain a high degree of reliability (> .7), suggesting that although the items within this construct were grouped into a single factor, they indicate accuracy and predictability of the data collection instrument. The results indicate that all the values of the five constructs are excellent (> 0.9=excellent, > 0.8=good) according to George and Mallery (2003).

Table 37: Cronbach Alpha for Internal Reliability (Empirical)

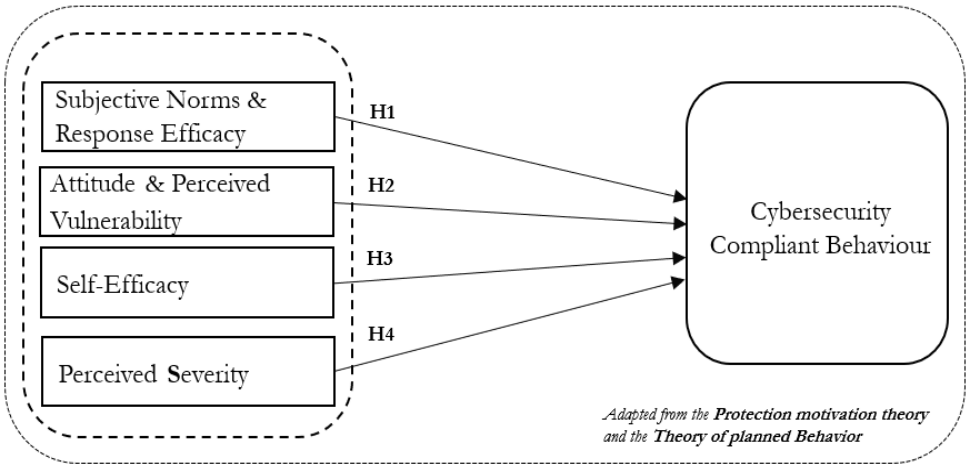
Construct	Code	α Before Adjustment	No. of items	Items Deleted	α After Adjustment
Subjective Norms & Response Efficacy	SNRE	.951	8	-	.951
Attitude & Perceived Vulnerability	ATTPV	.961	9	-	.961
Self-Efficacy	SE	.913	4	-	.920
Perceived Severity	PS	.900	3	-	.900
Cybersecurity Compliant Behavior	CCB	.884	5	-	.884
Overall Scale *(All independent Items)*		.962	24	-	.962

4.13. Updated Model and Hypothesis

Based on the findings of EFA and the reliability for both the theoretical and empirical factors, the study could technically continue with the further hypothesis testing with regression testing. However due to the high correlations between "*Subjective Norms"* and "*Response Efficacy*", and "*Attitude"* and *"Perceived Vulnerability"*, multicollinearity

issues could be encountered in the regression analysis when testing the relationships between the constructs, therefore the use the empirical factors will be used for the updated (Figure 6) model and hypothesis (Pallant, 2009).

Figure 6: New Model for Regression Analysis.



The constructs of "*Subjective Norms & Response Efficacy*", *"Attitude & Perceived Vulnerability*", "*Self-Efficacy"* and "*Perceived Severity"* have been identified as the determinants to "*Cybersecurity Compliant Behaviour".*

Hypothesis H1: *"Subjective Norms & Response Efficacy"* has a positive influence on "*Cybersecurity Compliant Behaviour".*

Hypothesis H2: *"Attitude & Perceived Vulnerability*" has a positive influence on "*Cybersecurity Compliant Behaviour".*

Hypothesis H3: Employee's "*Self-Efficacy"* will have a positive influence on "*Cybersecurity Compliant Behaviour".*

Hypothesis H4: Employee's "*Perceived Severity"* will have a positive influence on "*Cybersecurity Compliant Behaviour".*

4.14. Descriptives on Scales

Table 38 captures the newly extracted factors that influence correct cybersecurity behaviour while in a work-from-home setting. The *"Subjective Norms and Response Efficacy"* construct exhibited a mean score of 4.545 and a standard deviation of .775, which stills maintains a highly positive result and can be depicted as between "Somewhat Agree" and "Strongly Agree". The dependent variable *"Cybersecurity compliant Behaviour"* yielded the lowest mean of 4.371 with a standard deviation of .776, but still hovers above "Somewhat Agree". To summarise, all constructs are highly positive showing that employees fundamentally follow the corrective actions to security behaviour.

Table 38: Scale Descriptives

	N		Mean	Median	Std. Deviation	Minimum	Maximum
	Valid	Missing					
Subjective Norms & Response Efficacy	132	0	4.545	4.875	.775	1.25	5.00
Attitude & Perceived Vulnerability	132	0	4.611	5.000	.827	1.00	5.00
Self-Efficacy	132	0	4.254	4.500	.953	1.00	5.00
Perceived Severity	132	0	4.518	5.000	.989	1.00	5.00
Cybersecurity Compliant Behavior	132	0	4.371	4.600	.766	1.00	5.00

4.15. Statistical Hypothesis Testing Between Variables

This sub-section firstly presents the handling and test verification for the statistical assumptions (Section 3.5), prior to conducting a multiple regression analysis. Thereafter multiple linear regression was conducted to test the hypothesis (Section 4.15.4), followed by a summary of statistical hypothesis testing between variables (Section 4.15.5).

4.15.1. Statistical assumptions

4.15.1.1. Outliers

Appendix C (Table 56) indicates that the model's Regression Standardized Residuals fall outside of the advised range of -3.29 and +3.29 (Field, 2013). Furthermore, the histogram presented in Appendix C (Figure 7) noted outliers, and Appendix B (Figure 8) indicates the histogram after eliminating these cases to improve the model fit. Based on standard

residuals, two case were removed from the dataset. Thereafter the Standardized Residuals were within the advised ranges as indicated in Table 39 below. The Cook's Distance (Cook's value < 1.0), which determines the influence of an observation in regression, indicated that no outliers had a major influence in the data (Tabachnick et al., 2013). The final regression analysis will be conducted using the dataset of N = 130.

Table 39: Residual Statistics (Outliers Removed)

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.55	4.78	4.39	.604	130
Std. Predicted Value	-4.709	.642	.000	1.000	130
Standard Error of Predicted Value	.046	.239	0.077	.043	130
Adjusted Predicted Value	1.39	4.78	4.39	.606	130
Residual	-1.326	.882	.000	0.44	130
Std. Residual	**-2.966**	**1.971**	.000	.984	130
Stud. Residual	-3.054	2.023	.003	1.006	130
Deleted Residual	-1.406	.929	.003	0.46	130
Stud. Deleted Residual	-3.162	2.049	.000	1.014	130
Mahal. Distance	.383	35.965	3.969	6.712	130
Cook's Distance	.000	.129	.009	0.02	130
Centered Leverage Value	.003	.279	.031	.052	130

4.15.1.2. Multicollinearity

Table 40 indicate the result for the collinearity tests on SPSS, where the Variance Inflation Factor (VIF) for all constructs where <10 (Myers, 1990; Pallant, 2009) and Tolerance values above .1 (Menard, 2002) resulting in no issues regarding multicollinearity. In addition, the Condition index was evaluated for any values above 30 according to Field (2013) and this also suggests that there are no serious collinearity issues. Lastly there were no Variance Proportions >.90 (Pallant, 2009) of any values of the same dimension, suggesting no multicollinearity issues. The Condition index and various proportions are present in Appendix B Table 55

Table 40: Collinearity Coefficients

	Collinearity Statistics	
	Tolerance	VIF
Subjective Norms & Response Efficacy	.395	2.532
Attitude & Perceived Vulnerability	.322	3.105
Self-Efficacy	.489	2.044
Perceived Severity	.601	1.663

a. Dependent Variable: *Cyber security compliant Behaviour*

4.15.1.3. Sample Size

According to Field (2013), the common rules for most studies suggest 10-15 cases for each predictor variable In this study, six predictor variables were used in the conceptual framework, and four predictors in the updated model. With this suggestion 15:1, the minimum sample size required is 60 cases. A total of 188 responses were captured in Qualtrics, however this study utilized 132 viable responses which is more than the minimum required.

4.15.1.4 Linearity

To confirm linearity, a visual inspection of the scatterplots was done and is presented in Appendix C Figure 9. There is no obvious indication of non-linearity in these graphs, therefore according to Tabachnick et al. (2013) our assumption of linearity is met. Field (2013) also suggests that if a model is non-linear, the generalisation of the results is inhibited.

4.15.2. Correlation Results

The Pearson correlation coefficients for the newly created tool focus variables are shown in Table 40, and they were utilized to examine the relationships between the variables. The newly generated components identified using exploratory factor analysis, which are described in the section 4.10. The positive coefficient values show that the associated variable's mean tends to rise as one variable's value rises. The value (*r*), denotes the intensity of the relationship (the closer to 1, the stronger the relationship; 0 = no relationship), and as indicated Table 40, all value are prefixed with "+", specifies the direction of the relationship

There was a significant relationship between the dependant variable, "*Cybersecurity Compliant Behaviour"* and independent variable "*Subjective Norms & Response Efficacy"*, and a very strong positive correlation (r = .803) and significant (p(one-tailed) < .005.) The construct *"Attitude & Perceived Vulnerability"* also demonstrated a strong correlation with "*Cybersecurity Compliant Behaviour"* (r = .631, p < .005.).

Lastly, the *"Cyber security compliant Behaviour"* construct indicated a moderate positive correlation with both "*Self-Efficacy*" (r = .495) and "*Perceived Severity"* (r = .497) which was also statically significant (*p < .005).*

There is evidence of positive correlation between the independent variables "*Subjective Norms & Response Efficacy"* and *"Attitude & Perceived Vulnerability" (r=.704)* , however the values do not exceed the advisable cut-off of *r* = .90 as suggested by Field (2013) or *r*=0.8 by Senaviratna and A Cooray (2019) with suggest no multicollinearity issues. Further analysis will be done in the next section to identify if multicollinearity is a concern, however based on the Pearson correlation and significant values below, all constructs can be used in the model. In summary, all independent variables have a positive correlation with the dependant variable and are all statistically significant (p < .005)

Table 41: Pearson Correlation for All Constructs

		Cyber security compliant Behavior	Subjective Norms & Response Efficacy	Attitude & Perceived Vulnerability	Self-Efficacy	Perceived Severity
Pearson Correlation	Cyber security compliant Behavior	1.000	.803	.634	.495	.497
	Subjective Norms & Response Efficacy	.803	1.000	.742	.616	.531
	Attitude & Perceived Vulnerability	.632	.742	1.000	.664	.575
	Self-Efficacy	.495	.616	.664	1.000	.257
	Perceived Severity	.497	.531	.575	.257	1.000
Sig. (1-tailed)	Cyber security compliant Behavior		.000	.000	.000	.000
	Subjective Norms & Response Efficacy	.000		.000	.000	.000
	Attitude & Perceived Vulnerability	.000	.000		.000	.000
	Self-Efficacy	.000	.000	.000		.002
	Perceived Severity	.000	.000	.000	.002	

4.15.3. Overall fit of the model

4.15.2.1 Model Summary

The R^2 in the model presented in Table 42 indicates that the predictor variables *"Subjective Norms & Response Efficacy"*, *"Attitude & Perceived Vulnerability", "Self-efficacy"* and "*Perceived Severity*" explains 65.3% of the variation in the dependent variable *"Cybersecurity Compliant Behaviour"*.

Table 42: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.808[a]	.653	.642	.447

a. Predictors: (Constant), *Perceived Severity, Self-Efficacy, Subjective Norms & Response Efficacy, Attitude & Perceived Vulnerability*
b. Dependent Variable: *Cyber security compliant Behaviour*

4.15.2.2. ANOVA results

The ANOVA results presented in Table 43 indicate the model significance in predicating the dependent variable. used to assess the statistical significance of the regression model. The p value = < .001 indicates that the four predicator variables are jointly significant in explaining the dependent variable.

Table 43: ANOVA results

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	46.991	4	11.748	58.744	<,001[b]
	Residual	24.998	125	.200		
	Total	71.989	129			

a. Dependent Variable: *Cyber security compliant Behaviour*
b. Predictors: (Constant), *Perceived Severity, Self-Efficacy, Subjective Norms & Response Efficacy, Attitude & Perceived Vulnerability*

4.15.4. Multiple Linear Regression

A standard multiple linear regression was used to verify the strength of the relationship between the independent variables *"Subjective Norms & Response Efficacy", "Attitude & Perceived Vulnerability*", *"Self-Efficacy"* and "*Perceived Severity"* and the dependent variable "*Cybersecurity Compliant behaviour*". The regression was done using the four empirical factors yielded by the factor extraction. According to Pallant (2009), preliminary investigations were performed to confirm that the assumptions of multicollinearity, linearity, and outliers were not violated.

Table 44: Multiple Regression Model Summary

Constructs	Unstandardized Coefficients		Standardized Coefficients	95,0% Confidence Interval for B			
	B	Std. Error	Beta	Lower Bound	Upper Bound	t	Sig.
(Constant)	.498	.265		-.026	1.022	1.882	.062
Subjective Norms & Response Efficacy	.741	.086	.724	.571	.911	8.627	**.000**
Attitude & Perceived Vulnerability	.052	.088	.055	-.123	.227	.593	.554
Self-Efficacy	-.007	.060	-.009	-.126	.111	-.124	.902
Perceived Severity	.065	.053	.083	-.040	.169	1.228	.222

R^2 = .653. CI = confidence interval for B.
F-statistics: = 58.744 on 4 and 125 degrees of freedom, Sig. = .000, means p < .005

The model illustrates the R^2 in the regression model is .653, indicates that the predictor variables *"Subjective Norms & Response Efficacy"*, *"Attitude & Perceived Vulnerability", "Self-efficacy"* and "*Perceived Severity*" explains 65% of the variation in the dependent variable *"Cyber security compliant Behaviour".*

4.15.5. H1 – Influence of Subjective Norms & Response Efficacy to Cybersecurity Compliant Behaviour

The first hypothesis was to explore an employee's "*Subjective Norms & Response Efficacy*", during a work-from-home environment, and the influence on their "*Cybersecurity Compliant Behaviour".*

> ***H1o***: "*Subjective Norms & Response Efficacy*" has no influence on "*Cybersecurity Compliant Behaviour".*
>
> ***H1a***: "*Subjective Norms & Response Efficacy*" has a positive influence on "*Cybersecurity Compliant Behaviour".*

The multiple regression analysis as presented in Table 39, indicates that the construct *Subjective Norms & Response Efficacy* is significant predictor of "*Cybersecurity Compliant Behaviour"* where $B = .741$ and $p < .001$. Furthermore, the analysis revealed a strong positive association with the dependant variable, Therefore the new hypothesis H1 as explained in section 4.12 is supported.

4.15.6. H2 - Influence of Attitude & Perceived Vulnerability to Cybersecurity Compliant Behaviour

The second hypothesis was to explore an employee's *"Attitude & Perceived Vulnerability"* during a work-from-home environment, and the influence on their "*Cybersecurity Compliant Behaviour".*

> ***H2o***: *"Attitude & Perceived Vulnerability"* has no influence on "*Cybersecurity Compliant Behaviour".*
>
> ***H2a***: *"Attitude & Perceived Vulnerability"* has a positive influence on "*Cybersecurity Compliant Behaviour".*

The multiple regression analysis as presented in Table 39, indicates that the construct "*Attitude & Perceived Vulnerability*" was an insignificant predictor of "*Cybersecurity Compliant Behaviour"* where $B = .0521$ and $p = .554$. The analysis further revealed an insignificant positive association with the dependant variable, but according to the Pearson correlation, that is a strong correlation of "*Attitude & Perceived Vulnerability*" when tested in isolation. However, the regression model when all other variables are constant, showed insignificant. Therefore, statistically, the new hypothesis H2 is not supported.

4.15.7. H3 - Influence of Self-Efficacy to Cybersecurity Compliant Behaviour

The third hypothesis was to explore an employee's *"Self-Efficacy"* while in a work-from-home environment, and the influence on their "*Cybersecurity Compliant Behaviour".*

> ***H3o:*** Employee's *"Self-Efficacy"* will have no effect on "*Cybersecurity Compliant Behaviour".*
>
> ***H3a:*** Employee's *"Self-Efficacy"* will have a positive effect on "*Cybersecurity Compliant Behaviour".*

The multiple regression analysis indicates that the construct *Self-Efficacy"* is insignificant predictor of "*Cybersecurity Compliant Behaviour"* where $B = -.007$ and $p = .902$. Furthermore, the analysis also revealed that *Self-Efficacy"* has a strong positive

correlation with the dependant variable in isolation. Therefore, the new hypothesis H3 as explained in section 4.12 is not supported.

4.15.8. H4 - Influence of Perceived Severity to Cybersecurity Compliant Behaviour

The fourth hypothesis was to examine the extent of employee's "*Perceived Severity*" during a work-from-home environment, and the influence on their "*Cybersecurity Compliant Behaviour".*

> ***H4o***: Employee's "*Perceived Severity*" of threats, will have no influence on "*Cybersecurity Compliant Behaviour".*
>
> ***H4a***: Employee's "*Perceived Severity*" of threats, will have a positive influence on "*Cybersecurity Compliant Behaviour".*

The multiple regression analysis indicates that the construct "*Perceived Severity*" is an insignificant predictor of "*Cybersecurity Compliant Behaviour"* where $B = .065$ and $p = .222$. Therefore, the new hypothesis H4 as explained is not supported.

4.16. Chapter Summary

This research study examined how events, such as the Covid-19 work-from-home (WFH) policies and the subsequent remote or hybrid working conditions have influenced cybersecurity behaviour of employees in South Africa.

The statistical analysis commenced with a cleaned sample of 132 respondents that fit the criteria for work from home cultures. With this conceptual model fairly new, the first step was to perform an Exploratory Factor Analysis (EFA) to produce a reduced number of linear combinations (Section 4.10), if applicable. The initial framework consisted of 6 dependant variables, however based on the EFA results, the final model was reduced to four predictor constructs with a combination of items and a single dependent variable.

The correlational results also provided information about the form and degree of the relationships and showed that there was a significant relationship between the dependant variable, *"Cybersecurity Compliant Behaviour*" and independent variable *"Subjective Norms & Response Efficacy"* and yielded a very strong positive correlation which was

statistically significant. The construct *"Attitude & Perceived Vulnerability"* also demonstrated a strong correlation with *"Cybersecurity Compliant Behaviour"* in isolation. The *"Cybersecurity Compliant Behaviour"* construct indicated a moderate positive correlation with both *"Self-Efficacy"* and *"Perceived Severity"* which was also statically significant according to the Pearson's correlation.

The reliability and validity of the new constructs (both theoretical and empirical) and scales used were tested to establish a reliable factor structure and model. Furthermore, the new framework and hypothesis were amended according to the statistical results. (Section 4.12). This also included multiple tests to detect the possibility of multicollinearity among the explanatory variables before making any statistical conclusions.

Table 45 illustrates a summary of the regression results. The multiple linear regression analysis indicated that the predicator "*Subjective Norms & Response Efficacy"* had the strongest predictive capacity, while hypothesis H2, H3, H4 showed high positive relationships in isolation, are not supported where all variables remain constant.

Table 45: Hypothesis Summary Table

	Hypothesis	B	t	*p*	Result
H1	**"Subjective Norms & Response Efficacy" to Cybersecurity compliant Behaviour**	**.741**	8.627	**.000**	**Supported**
H2	"Attitude & Perceived Vulnerability" to Cybersecurity compliant Behaviour	.052	.593	.554	Not supported
H3	"Self-Efficacy" to Cybersecurity compliant Behaviour	-.007	-.124	.902	Not supported
H4	"Perceived Severity" to Cybersecurity compliant Behaviour	.065	1.228	.222	Not supported

5. DISCUSSION OF RESEARCH FINDINGS

This chapter presents the research findings discussed in Chapter 4 by using the established theoretical frameworks proposed in Chapter 2 in conjunction with the conceptual framework. The literature review presented in Chapter 2 will also form the foundation in comparison to the findings on the predictors of Cybersecurity Compliant Behaviour. Furthermore, the chapter addresses the results of each hypothesis and finally provides a summary and conclusion of the findings.

5.1. Brief Contextual Background

During the pandemic lockdown, the South African government instituted emergency policies to perpetuate work-from-home adoption. The lockdown ended in 2021, but the hybrid model, according to a recent survey by Microsoft, 88% of leaders' at large enterprises in South Africa will continue to adopt a more hybrid way of working on a permanently basis The dataset also reflects a similar statistic, as 76% of participants are still in a hybrid model post lockdown.

The hybrid working paradigm has been implemented as a solution, but it has consequences for cybersecurity in the context of remote work. The foundation of the study was designed to evaluate employee behaviour when working environments are suddenly affected by work-from-home policies and how an employee's behaviour transposes to a different location. It is important to note that the framework for this study, while taking previous studies in consideration is fairly new with regards to a remote working environment.

This research study sought to determine how *Cybersecurity Compliant Behaviour* are influenced by the effects of lockdown and remote working, caused by the Pandemic. The primary goal of the study was to better understand the predictors that influence *Cybersecurity Compliant Behaviour* in South Africa. Therefore, the new framework for this study incorporated two theoretical models, namely, the Protection Motivation theory (PMT) and the Theory of Planned Behaviour (TPB) to examine the relationships between the predictor variables (*"Subjective Norms & Response Efficacy", "Attitude & Perceived Vulnerability*", *"Self-Efficacy"* and "*Perceived Severity")* and the outcome variable *(Cybersecurity compliant Behaviour).*

This study aimed to provide insight on the two research objectives:

Research objectives

To examine the human aspect of cybersecurity compliant behaviour while assessing employee's individual behaviour traits in a remote working environment.

To investigate and assess the key factors that influence positive *Cybersecurity Compliant Behaviour* while working remotely, incorporating past literature on office-based cybersecurity behaviour.

5.2. Influence of Subjective Norms & Response Efficacy toward Cybersecurity Compliant Behaviour.

Subjective norms in this study, refers to a person's opinion of what people in their social and work environment value about the approach to compliant cybersecurity behaviour. It also refers to the notion that normative ideas are those that are established as a result of social pressure(Ajzen, 1985) and acts as a behavioural predictor. According to research by Anderson and Agarwal (2010) on home computer security, subjective norms were a key factor in preventing unauthorized access to computers.

Response efficacy is regarded as a unique personality attribute that can be effective in examining the relationship between behavioural intentions and specific cybersecurity behaviours(Shappie et al., 2020). Response efficacy alludes to the steps that employees will take to prevent security breaches and to reduce or mitigate data breaches while working from home. These actions may include, consciously installing frequent software updates, antivirus programs, applying firewalls and routine software patches as advised by the software vendor's or their internal IT departments. Past studies have identified that employees are more likely to perpetuate correct cybersecurity behaviour if the actions are associated with a positive view from their work colleagues and peers (Hanus & Yu, 2016). Similarly, a study by Torten et al. (2018) examined the impact of security awareness amongst IT professionals in Australia, showed that *Response Efficacy* provided the strongest influence on security behaviour.

To assess employees "Subjective Norms & Response Efficacy", and the influence on Cybersecurity Compliant Behaviour, while in a remote working context, this study focused on the employee's views of peer recommendations within the organisation (Management, IT, Co-workers, and Subordinates) while contrasting this with actionable corrective behaviour in mitigating security breaches. The regression model presented in Chapter 4 (Table 39) shows that *"Subjective Norms & Response Efficacy"* (*B = .741, p < .001*) has a positive relationship and was a significant predictor of *"Cybersecurity Compliant Behaviour"*. The beta coefficient for *"Subjective Norms & Response Efficacy"* indicates the degree of change in *"Cybersecurity Compliant Behaviour"* for every 1-unit of change in the "*Subjective Norms & Response Efficacy"* predictor variable. The standardized coefficient also indicates that this predictor has the highest relative importance among all the predictors variables..

There have been many comparative studies, however these studies were prior to the global lockdown and focused on either office-based or student participants. These findings are consistent with the findings of Torten et al. (2018) and Hanus and Yu (2016), but the results in this study indicate a stronger effect of the predictor variable. This may suggest that during lockdown, expedited security awareness and training within South African organisations have been vastly improved to provide adequate cybersecurity knowledge in a remote working context. In a study by Li et al. (2019), regarding the impact of cybersecurity policy awareness on employees, the authors assessed an employee's response efficacy with prior experience in cybersecurity practices. These studies concluded, that through the use of the PMT model, Response Efficacy directly influences cybersecurity behaviour. As discussed in Section 4.2 to 4.11 this study revealed that 85.2% of the respondents indicate taking the necessary measures to protect against unlawful security breaches, while 86.4% agree to social influence, and the benefits to cybersecurity compliant behaviour.

These findings illustrate that employees are more knowledgeable about security concerns and solutions than in the past, demonstrating a strong security culture and familiarity with information technology, thus resulting in better protecting company data assets. Overall, *"Subjective Norms & Response Efficacy"* play fundamental roles in modelling individuals *"Cybersecurity Compliant Behaviour"* by influencing their perceptions of social views about the effectiveness of correct security measures.

5.3. Influence of Attitude and Perceived Vulnerability toward Cybersecurity Compliant Behaviour.

Many behavioural studies have incorporated Attitude as a key construct to explore behavioural intention (Anderson & Agarwal, 2010; Nunes et al., 2021; Shropshire et al., 2015) to determine cybersecurity behaviour prior to the pandemic. Therefore, one of the main justifications for using Attitude in this study, is that it offers a suitable gauge to determine if liking or disliking a specific behaviour can change an employee's beliefs. Furthermore, a recent study by Wong et al. (2022) discussed the relation between cybersecurity awareness and Perceived vulnerability, where people with cyber security awareness and their underlying attitude will choose much more wisely in regards to perceived vulnerability since they are aware of the dangers and negative results. This also empirically explains why the two individual constructs (*Attitude and Perceived Vulnerability*) were combined during the statistical analysis in Section 4.10.1.

Psychology and related field research have demonstrated that emotion has a significant impact on people's attitudes about cybersecurity and their motivation and perception of their capacity to handle it, and finally their subsequent behaviours (Bagozzi et al., 2000).

The research findings for *"Attitude & Perceived Vulnerability"* demonstrated a strong positive association with *"Cybersecurity Compliant Behaviour*", however statistically insignificant. It is apparent from the descriptive statistics of this study that most employees (92.1%) have a positive attitude towards cybersecurity compliant behaviour and are conscious of their vulnerability in a remote working scenario if not adhering to corrective behaviour. There are many studies showing the similar results for the individual variables. One of the main conclusions from the recent study by Hadlington (2018) showed that attitudes towards cybersecurity was negatively correlated to the frequency with which they engaged in risky cybersecurity behaviours. The results for the construct contradict the findings by Li et al. (2019), where the authors showed "*Perceived Vulnerability"* as a single significant predicator of cybersecurity behaviour, and the study used the theoretical PMT theory without the inclusion of the TPB. Although the results from the regression contradict the views of some past studies, the model used in this study is a newly formulated framework to determine the factors that influence "*Cybersecurity Compliant Behaviour*".

5.4. Influence of Self-efficacy toward Cybersecurity Compliant Behaviour.

It refers to an employee's belief in their ability to successfully safeguard company data assets and information, and in the context of this research follow best practices to comply with recommended security practices. Past studies have indicated that *"Self-Efficacy"* has a significant influence on a person's capability to carry out or complete a task (Donalds & Osei-Bryson, 2020). This study aimed to gather employees retrospective view and confidence levels pertaining to their security competence.

According to the findings, 31.8% (Somewhat Agreed) and 53.8% (Strongly Agreed) of respondents had the expertise to adopt preventative measures to migrate cyber risks, accounting for more than 86% of all respondents. Furthermore, only 10% of respondents believe they are unprepared to deal with cyber risks. There is a distinct shift in Self efficacy from other pre-Covid cybersecurity studies, as employees have a positive perception about their own self-efficacy and the subsequent effectiveness of responses to cyberthreats.

The research findings for *"Self-Efficacy"* showed that this predictor has a coefficient ($B = -.007$, $p = .902$) that demonstrates a weak negative association with the dependent variable. The standardized coefficient, implied that this predictor has minimal importance in influencing "Cybersecurity Compliant Behaviour".

5.5. Influence of Perceived severity toward Cybersecurity Compliant Behaviour.

Perceived severity is meant to capture an employee's perception of a security incident. It raises employee's awareness of the potential risks while working remotely. If they understand the severe consequences of a security incident, such as reputational damage to the organisation or financial loss, they are more motivated to engage in secure online practices. The cybersecurity incident may have serious implications in a remote working scenario, however individual employees' workers may see the severity or scope of the incident differently.

In this study, the results show that while *"Perceived Severity"* is insignificant in predicting *"Cybersecurity Compliant behaviour"* however there is still a moderate positive correlation. Basically, the perception of threats could be a strong positive predictor if considered in isolation. The results confirm the findings in past studies by Ng et al. (2009) and Li et al. (2019), where *"Perceived Severity"* where insignificant. Previous studies have also speculated that this may be due to a lack of employee awareness to the magnitude of security incidents, however the results in this study showed an 88.4% of respondents are knowledgeable when assessing the consequences of security breaches via their local computers. The empirical findings indicate that when employees perceive the severity of a threat as high, they are more likely to adhere to recommended security measures. They are more inclined to use secure, strong, and unique passwords, make use of multi-factor authentication, regularly update their software, and use reputable software. Safa et al. (2015) conducted a similar study using the PMT theory, and the results showed the construct *"Perceived Severity*" as a significant predictor, but the differentiating component was the target population consisting of Information Security and Technology Experts. This sample frame would have affected the outcome, considering that all respondents where in the cybersecurity and technology sectors.

The empirical findings indicates that the construct "*Perceived Severity*" have a positive relationship but is an insignificant predictor towards "*Cybersecurity Compliant Behaviour"* (*B = .065, p = .222).* While the results show *"Perceived Severity*" as insignificant, based on the overarching responses indicate that 88.4% of respondents agree to correctly accessing the severity of a security incident,

5.6. Summary and Conclusion of Research Findings

The research paper presents the empirical findings of factors that influence cybersecurity compliant behaviour for employees that were forced into a work-from-home environment and have evolved into a hybrid mode of working. An online questionnaire was developed to assess their perceptions and views regarding the four predictors derived by factor analysis *("Subjective Norms & Response Efficacy", "Attitude & Perceived Vulnerability", "Self-Efficacy" and "Perceived Severity"*). Each question was crafted to specifically capture security culture factors in the attempt to evaluate the current risk status associated with remote work, from a non-technological perspective. The

framework developed for this study was grounded on two theoretical frameworks that have been widely used for cybersecurity behavioural analysis, namely Protection Motivation Theory and the Theory of Planned Behaviour.

This study confirmed correlation between behavioural traits and positive cybersecurity behaviour, as described in past studies, however the most significant determinant was identified as "*Subjective Norms & Response Efficacy*". This single construct consists of a combination of 8 items explained 73% of the variability of Cybersecurity Compliant Behaviour. While the results were founded on statistical analysis, it should be noted that within all constructs, the mean responses hovered around agree and strongly agree. This indicates a strong positive attitude towards cybersecurity where employees are much more aware of security risks and countermeasures than pre-lockdown. This also proves a robust focus by leadership of South African organisations in instituting a security culture to address the growing risk in cyberspace while in a remote context. As a result, remote employees are better equipped to deal with cyber risks, and consciously perform the required actions to protect company data assets and ensure privacy.

Furthermore, the constructs for "*Attitude & Perceived Vulnerability", "Self-Efficacy" and "Perceived Severity"* were not significant predictors but showed a highly positive correlation to Cybersecurity Compliant Behaviour. If the study is replicated, the results may differ as the sample size, and industries should be expanded for future research. The benefit of this study was to provide South African business leaders with a foundation of understanding how employee cybersecurity behaviours change without the constant engagement from peers and management regarding cybersecurity in an office environment. Furthermore, the model and questionnaire can form a foundation for evaluating employee's current awareness and adjust the formal training requirements accordingly.

6. RECOMMENDATIONS AND LIMITATIONS

This chapter presents the recommendations for organisational leaders with alignment of the rationale of this study. It also provides suggestions for future researchers in South Africa in Section 6.1.2. Finally, Section 6.2 discusses the limitations of the study, followed by the conclusion.

6.1. Recommendations For Organisations

Cybersecurity was a major focus during the pandemic, and with the increase of remote or hybrid models in South Africa the ownership of protecting organisational data assets typically rests with management. This study recommends that leadership in both public and private sectors should frequently engage on cybersecurity, thus sharing knowledge and developing policies and procedures that will encourage employees in all spheres to follow cybersecurity compliant behaviour.

Past studies, in behavioural security utilizing both qualitative and quantitative approaches, suggest that even formal cybersecurity training offered by employers do not pursue a user friendly, insightful format for employees. In order for employees to adjust personal preferences and behavioural traits associated with positive actions toward cybersecurity compliant behaviour, the information and training must adhere to a simplistic, informative format to clearly instruct and ensue adherence to security policies. Technical jargon should be carefully communicated in an insightful and intuitive manner.

6.2. Recommendations For Researchers

South Africa’s growth in remote work adoption is evident, and behavioural cybersecurity research helps policymakers and regulators design effective rules and regulations. Understanding the behavioural aspects that influence cybersecurity practices aids in the development of legislation that are compatible with users' habits, motives, and privacy concerns. This can encourage compliance and promote a safe and secure digital environment within all industries in South Africa. Furthermore, this study was based on an exploratory analysis an attempt to distinguish the key constructs that influence cybersecurity compliancy. The suggestion is to adapt the instrument and model to add more predicators to finalise a model that can be users by employers and policy makers.

This research sought to develop a simple framework based on pre-Covid studies and theoretical models to gather information to supplement leadership initiatives in South Africa within the cybersecurity domain. In the context of remote work and cybersecurity, there are several potential areas of future research, that can assist the private and public sectors in addressing emerging challenges and enhance the security by improving employee behaviour.

It would be advisable to include a moderating variable of organisation training within the framework. Thereafter, conduct a longitudinal study, evaluating the evolutionary results over time to show the benefit of cybersecurity training initiatives, and the inherent effect on employee behaviour.

Lastly, this study focused on a quantitative design and employees working remotely. Future research, including qualitative findings on how C-Suite levels within South African organisations address human issues of cybersecurity in the remote working context will further provide a richer understanding of cybersecurity compliant behaviour.

6.3. Limitations

The possible limitation for this study refers to non-probability sampling (convenience sampling) which suggests that it is impossible to establish a correct representation of the population (Bairagi & Munot, 2019). The raw data could be attributed to specific industries or geographic locations that may skew the results. The results show that this study was conducted on a sample composed of mostly respondent in a technology field, may either suggest that work-from-home cultures have predominantly been instituted in these specific fields. Furthermore, the technology field in South Africa may have better exposure to cybersecurity training and information.

This study gathered data of 186 respondents and 132 valid cases met the criteria during the statistical analysis. The lower-than-expected sample was also affected by the time constraints and lack of responses. It is advisable to expand the data collection over various other industries in South Africa, gathering data in both public and private sectors.

The new model, research instrument and scales possibly do not cover all the behaviour traits that may be significant in cybersecurity compliancy studies. A resulting limitation

was the insignificance of Attitude, and Perceived Severity and Vulnerability, however this could be attributed to the sample size and the industries.

There are also possible some limitations in terms of personality traits regarding anxiety and defensive mechanisms, as the topic of study relates to personal cybersecurity behaviour(Wong et al., 2022). Participants may feel pressured into providing responses that are deemed correct behaviour.

A drawback to cross-sectional research is that it makes it impossible to measure changes because the data is collected at a given time(Kumar, 2019). However, as this study is to determine the effects of remote work on security behaviour, data collection within a time-specific period is more pertinent for the research objectives.

An administrative limitation was the time frame for data collection. This period ranged from January to March 2023, after ethics approval, and the responses within the different provinces were limited and not as expected.

6.4. Conclusion

The present study aimed to address two associated objectives, firstly to identify the constructs that influence the correct cybersecurity behaviour of employees in a work from home environment and assess the predictive capacity of each of these behavioural conditions. The overarching sentiment from the sample size has informed the research instrument and the new framework through the lens of the Theory of Planned Behaviour and the Protection Motivation Theory, and the overall results show a positive outlook of cybersecurity in the context of remote work. All constructs show a highly positive outlook in mitigation of cyber risks, while employee's response efficacy to threats, coupled with the normative views of their peers being the largest predictive contributor. This study did advance the understanding of remote work culture from the perspective of cybersecurity awareness in South Africa and will provide a foundation for business leaders to evaluate current and future initiatives within the organisation. With the continuous evolution of cyberthreats, it is imperative that employee training and cybersecurity awareness continue within South African organisations, to effectively regulate behavioural and motivational aspects towards security consciousness.

REFERENCES

Abukari, A., & Bankas, E. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. *International Journal of Scientific and Engineering Research, 11*, 1401-1407.

Accenture. (2022). Cyber Threat Intelligence Report. https://www.accenture.com/za-en/insights/security/cyber-threat-intelligence

Africa, S. (2021). *Regulations and Guidelines - Coronavirus COVID-19*. South Africa Retrieved from https://www.gov.za/covid-19/resources/regulations-and-guidelines-coronavirus-covid-19

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In J. Kuhl & J. Beckmann (Eds.), *Action Control: From Cognition to Behavior* (pp. 11-39). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-69746-3_2

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

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in society, 73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Anderson, C., & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly, 34*, 613-643. https://doi.org/10.2307/25750694

Bagozzi, R. P., Baumgartner, H. R., Pieters, R., & Zeelenberg, M. (2000). The role of emotions in goal-directed behavior.

Bairagi, V., & Munot, M. (2019). *Research Methodology: A Practical and Scientific Approach*.

Baz, M., Alhakami, H., Agrawal, A., Baz, A., & Ahmad Khan, R. (2021). Impact of COVID-19 Pandemic: A Cybersecurity Perspective. *Intelligent Automation and Soft Computing, 27*, 641-652.

Beautement, A., Sasse, A., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. https://doi.org/10.1145/1595676.1595684

Bloom, N. (2014). To raise productivity, let more employees work from home. *92*(1-2), 28. https://go.exlibris.link/ZyWGjwsM

Borkovich, D., & Skovira, R. (2020). Working From Home: Cybersecurity in the Age of Covid-19. *Information Systems*, *21*, 234-236. https://doi.org/10.48009/4_iis_2020_234-246

Child, D. (2006). *The essentials of factor analysis*. A&C Black.

Conway, J. M., & Huffcutt, A. I. (2003). A review and evaluation of exploratory factor analysis practices in organizational research. *Organizational research methods*, *6*(2), 147-168.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Creswell, J., & Guetterman, T. (2018). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research, 6th Edition*.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *psychometrika*, *16*(3), 297-334.

Daoud, J. I. (2017). Multicollinearity and regression analysis. Journal of Physics: Conference Series,

Deloitte. (2020). COVID-19's Impact on Cybersecurity," 2020. https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/risk/ng-COVID-19-Impact-on-Cybersecurity-24032020.pdf.

Deo, P., Raj, G., & Perumal, R. (2021). How Covid-19 is Dramatically Changing Cybersecurity? https://www.tcs.com/perspectives/articles/how-covid-19-is-dramatically-changing-cybersecurity

DeVellis, R. F., & Thorpe, C. T. (2021). *Scale development: Theory and applications*. Sage publications.

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*, 102056-102016. https://doi.org/10.1016/j.ijinfomgt.2019.102056

ENISA. (2021). *ENISA Threat Landscape 2021*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Ferguson, P., & Huston, G. (1998). What is a VPN?

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Sage Publications.

Furnell, S., & Shah, J. N. (2020). Home working and cyber security – an outbreak of unpreparedness? *Computer Fraud & Security*, *2020*(8), 6-12. https://doi.org/https://doi.org/10.1016/S1361-3723(20)30084-1

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35*(2), 486-505. https://doi.org/10.1057/s41284-021-00286-2

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology*, *2*, 13-20.

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12*, 269-281. https://doi.org/10.5281/zenodo.1467909

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52-65. https://doi.org/https://doi.org/10.1016/j.cose.2016.12.016

Hancock, J. (2022). Understand The Mistakes That Compromise Your Company's Cybersecurity. https://www.tessian.com/resources/research-report-why-do-people-make-mistakes/

Hanus, B., & Yu, W. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*, 2-16. https://doi.org/10.1080/10580530.2015.1117842

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/https://doi.org/10.1016/j.cose.2011.10.007

INTERPOL (Ed.). (2021). *African cyberthreat assesment report*. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa.

James, T., Nottingham, Q., & Kim, B. C. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information technology and management*, *14*(2), 69-89. https://doi.org/10.1007/s10799-012-0147-4

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic

Literature Review. *IEEE Access, 9*, 99339-99363. https://doi.org/10.1109/ACCESS.2021.3097144

Kumar, R. (2019). *Research Methodology - A step-by-step guide for Beginners* (4th ed.). Sage Publishing.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

Malwarebytes. (2020). Enduring from home - COVID-19's impact on business security. https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

McAfee, A., & Brynjolfsson, E. (2012). Big data: the management revolution. *Harv Bus Rev*, *90*(10), 60-66, 68, 128.

Menard, S. (2002). *Applied logistic regression analysis*. Sage.

Microsoft. (2020). New research reveals future work trends for South African organisations. https://news.microsoft.com/en-xm/2020/11/12/new-research-reveals-future-work-trends-for-south-african-organisations/

Myers, R. H. (1990). *Classical and modern regression with applications* (Vol. 2). Duxbury press Belmont, CA.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825. https://doi.org/https://doi.org/10.1016/j.dss.2008.11.010

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. (1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nunes, P., Antunes, M., & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science*, *181*, 173-181. https://doi.org/https://doi.org/10.1016/j.procs.2021.01.118

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1.

Omorog, C. D., & Medina, R. P. (2020). Internet Security Awareness of Filipinos. *International Journal of Computing Sciences Research*, *1*(4), 14-26. https://doi.org/10.25147/ijcsr.2017.001.1.18

Considerations for implementing and adjusting public health and social measures in the context of COVID-19, (2021). https://www.who.int/publications/i/item/considerations-in-adjusting-public-health-and-social-measures-in-the-context-of-covid-19-interim-guidance

Pallant, J. (2009). *SPSS survival manual: a step-by-step guide to data analysis using SPSS version 15*. Open University Press.

Pallant, J. (2020). *SPSS survival manual: a step by step guide to data analysis using IBM SPSS* (7th ed.). McGraw-Hill Education. https://go.exlibris.link/St5XkGVl

Pallant, J., & Manual, S. S. (2007). A step by step guide to data analysis using SPSS for windows version 15. *SPSS Survival manual*, *3*.

Pham, M. (2021). Remote Work Security Survey Results: Is Remote Work Really Secure? https://www.wrike.com/blog/remote-work-security-survey/

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826. https://doi.org/10.1016/j.cose.2009.05.008

Rogers, R., Cacioppo, J., & Petty, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In (pp. 153-177).

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *J Psychol*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

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. https://doi.org/https://doi.org/10.1016/j.cose.2015.05.012

Saunders, M., Lewis, P., Thornhill, A., & Bristow, A. (2019). "Research Methods for Business Students" Chapter 4: Understanding research philosophy and approaches to theory development. In (pp. 128-171).

Schindler, P. (2019). *Business Research Methods* (13th ed.). Mcgraw-Hill Rental.

Senaviratna, N., & A Cooray, T. (2019). Diagnosing multicollinearity of logistic regression model. *Asian Journal of Probability and Statistics*, *5*(2), 1-9.

Seymour, H. (2020). A pandemic and remote working: cyber security under the microscope. https://www.ifsecglobal.com/cyber-security/a-pandemic-and-remote-working-cybersecurity-under-the-microscope/

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475-480. https://doi.org/10.1037/ppm0000247

Shen, S., Chen, O., Sun, J., Mok, L., Gao, A., & Wan, D. D. K. (2020). Coronavirus (COVID-19) Outbreak: Short- and Long-Term Actions for CIOs. https://www.gartner.com/en/doc/720647-covid-19-outbreak-short-and-long-term-actions-for-cios

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191.

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. *International Cybersecurity Law Review*, *1*(1-2), 51-61. https://doi.org/10.1365/s43439-020-00014-3

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics, 5th ed*. Allyn & Bacon/Pearson Education.

Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2013). *Using multivariate statistics* (Vol. 6). pearson Boston, MA.

Tam, C., Conceição, C. d. M., & Oliveira, T. (2022). What influences employees to follow security policies? *Safety Science*, *147*, 105595. https://doi.org/https://doi.org/10.1016/j.ssci.2021.105595

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *Int J Med Educ*, *2*, 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79. https://doi.org/https://doi.org/10.1016/j.cose.2018.08.007

Treiblmaier, H., & Filzmoser, P. (2010). Exploratory factor analysis revisited: How robust methods support the detection of hidden multivariate data structures in IS research. *Information & management*, *47*, 197-207. https://doi.org/10.1016/j.im.2010.02.002

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Watkins, M. W. (2018). Exploratory Factor Analysis: A Guide to Best Practice. *Journal of Black Psychology*, *44*(3), 219-246. https://doi.org/10.1177/0095798418771807

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

APPENDIX A: DATA COLLECTION INSTRUMENT

Cover Letter for Research Instrument

Dear Sir / Madam

My name is Ravashalin Pather, and I am a Master of Management student at the Witwatersrand Business school. I would like to invite you to participate in my research study on the impact of work-from-home and hybrid mode on cybersecurity practices in South Africa.

This research study examines how events, such as the Covid-19 work-from-home policies have influenced cybersecurity practices of employees in South Africa.

Information regarding completing the survey:

1. It should take approximately 8 to 10 minutes to complete the survey.
2. There is no personal information that will be collected; therefore, your identity will be anonymous.
3. Completion of the survey is voluntary.

Please feel free to contact me if you have any further questions and thank you for taking the time to complete the survey.

Your Sincerely

Ravashalin Pather
082 998 8584
1806289@students.wits.ac.za

Supervisor: Dr Kiru Pillay
E-mail: kiru2010@gmail.com

Research instrument

Informed consent

Q1 I hereby confirm that:

- I understand that I am under no obligation to complete the survey. (1)
- I give consent that my responses may be used for academic research. (2)
- I will answer the survey questions honestly and to the best of my knowledge. (3)

Demographics

Q2 Please indicate the province that you are currently living in.

- Gauteng (1)
- Free State (2)
- Limpopo (3)
- Mpumalanga (4)
- North West (5)
- KwaZulu-Natal (6)
- Eastern Cape (7)
- Western Cape (8)
- Northern Cape (9)

Q3 Please select your highest level of education.

- Primary/Secondary School (1)
- Certificate/Diploma (2)
- Bachelors/Honours Degree (3)
- Master's Degree (4)
- Doctoral Degree (5)

Q4 Please select the business domain of the organization you work for:

- Banking & Financial (1)
- Education & Research (2)
- Electrical Power & Energy Systems (3)
- Health (4)
- IT (Information Technology) (5)

- Public Sector (6)
- Transport (7)
- Security (cyber) (8)
- Telecommunications (9)
- Other (10)

Work from home status

Q5 During Lockdown, I was offered the opportunity to work from home via remote access?

- Yes (1)
- No (2)

Skip To: Q6 If During Lockdown, I was offered the opportunity to work from home via remote access? = Yes

Skip To: End of Survey If During Lockdown, I was offered the opportunity to work from home via remote access? = No

Q6 I am currently working from home or spend a part of my "work week" at home.

- Yes (1)
- No (2)

Self-Efficacy

Q7 I have the necessary skills to protect myself from information security violations while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8 I have the expertise to implement preventative measures to stop people from getting my confidential information in a work from home environment.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q9 I have the skills to implement preventative measures to stop people from damaging my computer while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q10 I believe that it is within my control to protect myself from information security violations while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Attitude

Q11 Information security awareness and behaviour is necessary while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q12 Information security awareness and behaviour is beneficial while working from home.

- Strongly disagree (1)

- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q13 Practicing information security behaviour while working from home is useful.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q14 I have a positive outlook on information security behaviour in a work from home environment.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q15 I believe that the information security awareness is valuable to any organization while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Perceived vulnerability

Q16 I feel that my organisation could become vulnerable to security breaches, if I don't adhere to its information security policy while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q17 I feel that I could fall victim to a malicious attack if I fail to comply with my organization's information security policy while working from home.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q18 I believe that my effort to protect my organisation's information will reduce illegal access to it, while working from home.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q19 My organization's data and resources may be compromised if I don't pay adequate attention to information security policies and guidelines while working from home.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Perceived severity

Q20 Having my computer infected by a virus as a result of opening a suspicious email attachment is a serious problem for me.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q21 At home, having my confidential information accessed by someone without my consent or knowledge is a serious problem for me.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q22 Losing my organisation's data from hacking is a serious problem for me while working from home.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Subjective Norms

Q23 My manager thinks that I should follow the organisation's cyber security policy while working from home.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q24 My co-workers think that I should follow the organisation's cyber security policy while working from home.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q25 My organisation's IT department pressures me to follow the organisation's cyber security policy while working from home.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q26 My subordinates think I should follow the organisation's cyber security policy while working from home.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Response efficacy

Q27 Antivirus software installation and regular updates are successful at preventing virus infections on my PC.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q28 Installation and frequent updates of antivirus software is effective in preventing virus infections on my computer.

- o Strongly disagree (1)
- o Somewhat disagree (2)
- o Neither agree nor disagree (3)
- o Somewhat agree (4)
- o Strongly agree (5)

Q29 Installation and configuration of firewall software on my computer is effective in preventing unwanted traffic on my computer.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q30 Applying security patches on my operating system (Windows or MAC) is an effective way of preventing hacker attacks on my computer while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Cybersecurity compliant behavior

Q31 I consider security experts recommendations in my information security manner while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q32 When working from home, and before taking any action that affects information security, I think about its consequences.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q33 I talk with security experts before I do something that relates to information security while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q34 I consider my previous experience in information security to avoid repeating prior mistakes while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q35 I always try to change my habits to security conscious behaviour while working from home.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither agree nor disagree (3)
- Somewhat agree (4)
- Strongly agree (5)

Consistency Matrix

Table 46 : Consistency Matrix

	HYPOTHESIS	CONSTRUCT	DATA SOURCE	VARIABLE	AUTHOR SOURCES
Cybersecurity Threat Assessment	Perceived severity has a positive influence on Cybersecurity Compliant Behaviours	Perceived severity	Q.20-Q.22 (Likert)	IV	Adapted from: (Li et al., 2019)
	Perceived vulnerability has a positive influence on Cybersecurity Compliant Behaviours	Perceived vulnerability	Q.16-Q.19 (Likert)	IV	Adapted from (Li et al., 2019)
Employee Response efficacy	Response-efficacy has a positive influence on Cybersecurity Compliant Behaviours	Response efficacy	Q.27-Q.30 (Likert)	IV	Adapted from (Hanus & Yu, 2016)
	Self-efficacy has a positive influence on Cybersecurity Compliant Behaviours	Self-efficacy	Q.7-Q.10 (Likert)	IV	Adapted from (Ifinedo, 2012)
Attitude	Employee's positive attitude has a positive influence on Cybersecurity Compliant Behaviours	Attitude	Q.11-Q.15 (Likert)	IV	Adapted from (Safa et al., 2015)
Subjective Norms	Employee's positive subjective norms, has a positive influence on Cybersecurity Compliant Behaviours	Subjective Norms	Q.23-Q.26 (Likert)	IV	Adapted from (Ifinedo, 2012)
		Cybersecurity Compliant Behaviour	Q.31 - .35 (Likert)	DV	Adapted from (Ifinedo, 2012)

Ethic Clearance Document

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/DB1806289/909
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	The impact of work from home and hybrid mode on cybersecurity practices in South Africa.
Investigator / Researcher	Mr Ravashalin Pather
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed anonymity and confidentiality.
Issue Date of Certificate	2022-12-20
Expiry date	Date of submission of the project / research report
Chairperson	Prof Anthony Stacey ☎ +27 11 717 3587 +27 82 880 4531 anthony.stacey@wits.ac.za

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.

I fully understand the conditions under which I am authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I undertake to resubmit the protocol to the Committee.

Signature

05-01-2023
Date:

APPENDIX B: EXPLORATORY FACTOR ANALYSIS

Table 47: Communalities for Cybersecurity Compliant Behaviour

	Initial	Extraction
CCB_Q31	.733	.811
CCB_Q32	.682	.728
CCB_Q33	.446	.463
CCB_Q34	.438	.461
CCB_Q35	.636	.713

Extraction Method: Principal Axis Factoring.

Table 48: Anti image (Cybersecurity Compliant behaviour)

	CCB_Q31	CCB_Q32	CCB_Q33	CCB_Q34	CCB_Q35
CCB_Q31	**.803**[a]	-0.524	-0.349	-0.048	-0.271
CCB_Q32	-0.524	**.835**[a]	-0.012	-0.121	-0.252
CCB_Q33	-0.349	-0.012	**.900**[a]	-0.098	-0.093
CCB_Q34	-0.048	-0.121	-0.098	**.902**[a]	-0.332
CCB_Q35	-0.271	-0.252	-0.093	-0.332	**.873**[a]

Table 49: Factor Matrix for Cybersecurity Compliant Behaviour

	Factor 1
CCB_Q31	.901
CCB_Q32	.853
CCB_Q33	.844
CCB_Q34	.681
CCB_Q35	.679

Extraction Method: Principal Axis Factoring.

a. 1 factors extracted. 5 iterations required.

Table 50: Communalities for Independent Variables

	Initial	Extraction
SE_Q7	.596	.579
SE_Q8	.798	.780
SE_Q9	.714	.724
SE_Q10	.722	.734
ATT_Q11	.951	.876
ATT_Q12	.927	.837
ATT_Q13	.877	.802
ATT_Q14	.751	.672
ATT_Q15	.864	.838
PV_Q16	.723	.549
PV_Q17	.780	.624
PV_Q18	.850	.791
PV_Q19	.787	.695
PS_Q20	.727	.669
PS_Q21	.796	.780
PS_Q22	.793	.868
SN_Q23	.866	.821
SN_Q24	.788	.653
SN_Q25	.691	.604
SN_Q26	.746	.678
RE_Q27	.877	.773
RE_Q28	.898	.806
RE_Q29	.859	.775
RE_Q30	.856	.757

Extraction Method: Principal Axis Factoring.

Table 51: Anti-image Matrices (Independent Variables)

	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30
Q7	.950[a]	-0.258	-0.162	-0.123	0.069	-0.016	-0.082	-0.152	0.026	0.058	-0.183	0.071	-0.027	0.023	0.090	-0.055	-0.116	-0.005	0.061	0.104	0.021	0.002	0.081	-0.067
Q8	-0.258	.870[a]	-0.322	-0.481	-0.269	0.149	0.239	0.166	-0.233	-0.024	-0.015	-0.023	0.227	-0.055	0.107	-0.027	0.130	0.191	-0.178	-0.201	0.039	-0.005	-0.002	-0.183
Q9	-0.162	-0.322	.958[a]	-0.199	-0.011	0.030	-0.031	0.014	-0.065	0.018	0.138	-0.144	0.020	-0.015	-0.063	0.057	-0.065	-0.075	0.119	-0.073	-0.072	-0.057	0.011	0.130
Q10	-0.123	-0.481	-0.199	.913[a]	0.140	-0.157	-0.119	-0.184	0.187	-0.007	-0.002	0.093	-0.157	0.056	-0.014	0.011	-0.090	-0.137	0.070	0.194	0.011	-0.005	-0.022	0.046
Q11	0.069	-0.269	-0.011	0.140	.896[a]	-0.686	-0.332	-0.225	-0.189	0.257	-0.147	0.175	-0.263	0.073	-0.120	0.000	-0.263	0.122	-0.086	0.098	0.026	0.031	0.141	-0.014
Q12	-0.016	0.149	0.030	-0.157	-0.686	.922[a]	-0.126	-0.013	0.014	-0.122	-0.018	-0.006	0.091	-0.092	0.123	-0.072	0.147	-0.094	0.143	-0.050	-0.099	-0.081	-0.230	0.236
Q13	-0.082	0.239	-0.031	-0.119	-0.332	-0.126	.922[a]	-0.044	-0.254	-0.213	0.207	-0.260	0.333	-0.120	-0.051	0.118	0.095	0.091	-0.109	-0.105	-0.003	0.095	0.102	-0.286
Q14	-0.152	0.166	0.014	-0.184	-0.225	-0.013	-0.044	.955[a]	-0.167	-0.011	0.017	-0.072	0.182	-0.033	0.026	0.017	0.066	0.067	-0.043	-0.194	0.175	-0.122	-0.220	0.107
Q15	0.026	-0.233	-0.065	0.187	-0.189	0.014	-0.254	-0.167	.937[a]	-0.091	0.035	-0.232	-0.246	0.212	-0.034	-0.022	0.069	-0.237	0.099	0.258	-0.154	0.104	0.094	-0.033
Q16	0.058	-0.024	0.018	-0.007	0.257	-0.122	-0.213	-0.011	-0.091	.895[a]	-0.524	0.231	-0.123	-0.335	-0.021	0.055	-0.101	0.045	-0.070	0.065	0.183	-0.194	0.041	-0.057
Q17	-0.183	-0.015	0.138	-0.002	-0.147	-0.018	0.207	0.017	0.035	-0.524	.898[a]	-0.546	0.017	0.053	0.007	0.022	-0.035	-0.015	-0.020	-0.075	-0.169	0.130	0.105	0.115
Q18	0.071	-0.023	-0.144	0.093	0.175	-0.006	-0.260	-0.072	-0.232	0.231	-0.546	.920[a]	-0.316	-0.121	-0.077	0.074	0.103	-0.091	-0.034	0.046	0.118	-0.141	-0.154	0.049
Q19	-0.027	0.227	0.020	-0.157	-0.263	0.091	0.333	0.182	-0.246	-0.123	0.017	-0.316	.920[a]	-0.275	0.200	-0.071	0.099	0.036	-0.133	-0.174	-0.033	-0.008	0.018	-0.202
Q20	0.023	-0.055	-0.015	0.056	0.073	-0.092	-0.120	-0.033	0.212	-0.335	0.053	-0.121	-0.275	.925[a]	-0.180	-0.216	-0.032	0.037	0.023	0.051	-0.134	0.202	0.077	-0.124
Q21	0.090	0.107	-0.063	-0.014	-0.120	0.123	-0.051	0.026	-0.034	-0.021	0.007	-0.077	0.200	-0.180	.836[a]	-0.748	0.124	-0.171	-0.020	-0.037	-0.034	0.075	-0.140	0.046
Q22	-0.055	-0.027	0.057	0.011	0.000	-0.072	0.118	0.017	-0.022	0.055	0.022	0.074	-0.071	-0.216	-0.748	.832[a]	-0.186	0.161	-0.040	0.028	0.057	-0.127	0.131	-0.018
Q23	-0.116	0.130	-0.065	-0.090	-0.263	0.147	0.095	0.066	0.069	-0.101	-0.035	0.103	0.099	-0.032	0.124	-0.186	.926[a]	-0.488	-0.359	-0.202	-0.055	-0.076	0.047	-0.162
Q24	-0.005	0.191	-0.075	-0.137	0.122	-0.094	0.091	0.067	-0.237	0.045	-0.015	-0.091	0.036	0.037	-0.171	0.161	-0.488	.918[a]	0.070	-0.358	0.033	0.072	-0.113	-0.003
Q25	0.061	-0.178	0.119	0.070	-0.086	0.143	-0.109	-0.043	0.099	-0.070	-0.020	-0.034	-0.133	0.023	-0.020	-0.040	-0.359	0.070	.951[a]	-0.157	-0.005	-0.022	-0.154	0.200
Q26	0.104	-0.201	-0.073	0.194	0.098	-0.050	-0.105	-0.194	0.258	0.065	-0.075	0.046	-0.174	0.051	-0.037	0.028	-0.202	-0.358	-0.157	.932[a]	-0.034	-0.007	0.054	-0.082
Q27	0.021	0.039	-0.072	0.011	0.026	-0.099	-0.003	0.175	-0.154	0.183	-0.169	0.118	-0.033	-0.134	-0.034	0.057	-0.055	0.033	-0.005	-0.034	.931[a]	-0.667	-0.157	0.045
Q28	0.002	-0.005	-0.057	-0.005	0.031	-0.081	0.095	-0.122	0.104	-0.194	0.130	-0.141	-0.008	0.202	0.075	-0.127	-0.076	0.072	-0.022	-0.007	-0.667	.924[a]	-0.139	-0.223
Q29	0.081	-0.002	0.011	-0.022	0.141	-0.230	0.102	-0.220	0.094	0.041	0.105	-0.154	0.018	0.077	-0.140	0.131	0.047	-0.113	-0.154	0.054	-0.157	-0.139	.929[a]	-0.545
Q30	-0.067	-0.183	0.130	0.046	-0.014	0.236	-0.286	0.107	-0.033	-0.057	0.115	0.049	-0.202	-0.124	0.046	-0.018	-0.162	-0.003	0.200	-0.082	0.045	-0.223	-0.545	.919[a]

Table 52: Communalities for 2nd Order Factor Analysis

	Initial	Extraction
Subjective Norms & Response Efficacy	.646	.769
Attitude & Perceived Vulnerability	.711	.894
Self-Efficacy	.530	.464
Perceived Severity	.437	.358

Extraction Method: Principal Axis Factoring.

Table 53: Factor Matrix for 2nd Order Factor Analysis

	Factor 1
Attitude & Perceived Vulnerability	.945
Subjective Norms & Response Efficacy	.877
Self-Efficacy	.681
Perceived Severity	.598

Extraction Method: Principal Axis Factoring.

a. 1 factors extracted. 10 iterations required.

Table 54: Anti-image Matrices (Cybersecurity Compliant Behavior)

	Subjective Norms & Response Efficacy	Attitude & Perceived Vulnerability	Self-Efficacy	Perceived Severity
Subjective Norms & Response Efficacy	.798[a]			
Attitude & Perceived Vulnerability	-0.430	.725[a]		
Self-Efficacy	-0.289	-0.448	.728[a]	
Perceived Severity	-0.261	-0.396	0.268	.724[a]

a. Measures of Sampling Adequacy(MSA)

Table 55: Collinearity Diagnostics

				(Constant)	Subjective Norms & Response Efficacy	Attitude & Perceived Vulnerability	Self-Efficacy	Perceived Severity
1	1	4.932	1.000	0.00	0.00	0.00	0.00	0.00
	2	0.033	12.222	0.01	0.00	0.00	0.33	0.39
	3	0.019	16.034	0.83	0.00	0.01	0.10	0.22
	4	0.009	23.068	0.15	0.46	0.16	0.52	0.34
	5	0.006	27.557	0.01	0.54	0.83	0.06	0.05

APPENDIX C: REGRESSION MODEL

Table 56: Residual Statistics (Outliers present)

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.89	4.73	4.37	0.571	132
Std. Predicted Value	-4.347	.620	.000	1.000	132
Standard Error of Predicted Value	.053	.276	.089	.049	132
Adjusted Predicted Value	1.67	4.74	4.37	.575	132
Residual	-2.140	1.981	.000	.511	132
Std. Residual	**-4.123**	**3.817**	.000	.985	132
Stud. Residual	-4.158	4.136	.003	1.011	132
Deleted Residual	-2.177	2.327	.003	.540	132
Stud. Deleted Residual	-4.457	4.429	.001	1.034	132
Mahal. Distance	.394	36.170	3.970	6.567	132
Cook's Distance	.000	.597	.012	.054	132
Centered Leverage Value	.003	.276	.030	.050	132

Figure 7: Histogram of Regression Standardise Residuals with Outliers

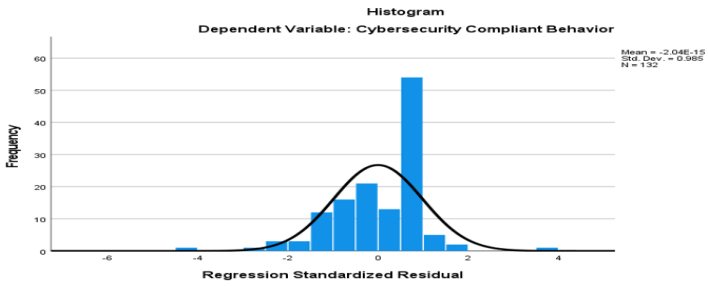


Figure 8: Histogram of Regression Standardise Residuals - Outliers Removed

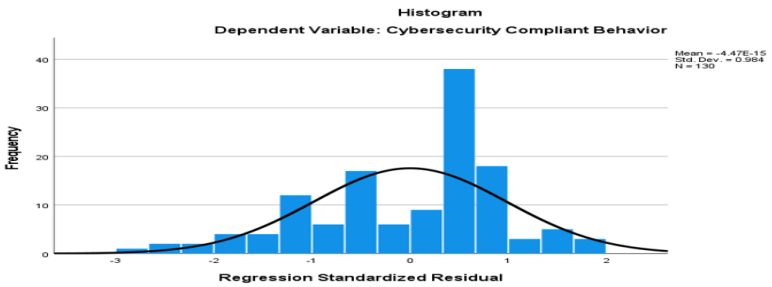


Figure 9: Scatterplot

