The influence of COVID-19 pandemic-induced contextual factors on information security policy compliance.

An empirical report presented to:

Department of Information Systems
University of Cape Town

Submitted by:

Popyeni Kautondokwa (KTNPOP001)
Research Supervisor: Zainab Ruhwanya
Research co-supervisor: Prof. Irwin Brown

In partial fulfilment of the requirements for the course:
Masters of Commerce (full-time) – Information Systems
(INF5000W)

Date: 22 May 2023

Plagiarism Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the APA Convention for citation and referencing. Each contribution to, and quotation from, the works of other people has been attributed, cited and referenced in this empirical report, *The influence of COVID-19 pandemic-induced contextual factors on information security policy compliance.*

3. I acknowledge that copying someone else's assignment or essay, or part of it, is wrong, and declare that this is my own work.

4. I have not allowed and will not allow another person or group to copy my work with the intention of passing it off as their own.

Signature: Signed by candidate **Date**: 22/05/2023

CONTENTS

TABLE OF FIGURES

LIST OF TABLES

Acknowledgement

I would like to express my heartfelt gratitude to my supervisors, Zainab Ruhwanya and Professor Irwin Brown, for their unwavering support, guidance, and invaluable feedback throughout my research project. Without their expertise and encouragement, this dissertation would not have been possible.

I would also like to extend my sincere appreciation to the Department of Information Systems at the University of Cape Town for their support and for providing me with the necessary resources to complete my research.

Furthermore, I would like to thank the almighty for facilitating this research project and for blessing me with the strength and perseverance to see it through to completion.

Finally, I would like to express my thanks to all those who have supported me in any way, whether through their encouragement, assistance, or words of wisdom. Your contributions have been instrumental in making this project a success, and I am truly grateful.

Abstract

This study aims to understand the impact of COVID-19 pandemic-induced contextual factors on information security policy compliance. The most significant change resulting from the COVID-19 pandemic has been a shift to working from home. Hence, this study aims to understand the impact that telecommuting has had on organisations' information security rules and procedures and how these rules and procedures have impacted the compliance behaviour of employees. This study was based on a conceptual model and used the quantitative research methodology. The sample population for this study was employees working in South African organisations that have information security policies. This study had 298 participants and the data was collected during the fourth wave of COVID-19 infections in South Africa using survey questionnaires. Analysis was conducted using Partial Least Squares Structural Equation Modelling.

This study found that technostress had a negative impact on the compliance behaviour of employees, while telecommuting had a positive impact on information security policy awareness and information security policy reviews within organisations. This study also found that information security policy awareness and information security policy reviews in organisations had a significant impact on the compliance behaviour of employees in organisations.

This study makes several contributions. Practical contributions include understanding the effect of the work-from-home arrangement on information security policy compliance behaviour, on information security policy awareness and on information security policy reviews. Theoretically, the study developed a conceptual model which can be used by researchers to understand compliance behaviour and to build on this research.

Findings from this study can be used by organisations with work-from-home arrangements to strengthen security awareness programs and to update existing information security policies. Further studies can be conducted to understand the impact of COVID-19 pandemic-induced contextual factors in other settings and geographical regions.

Keywords
Information security, COVID-19, compliance behaviour, information security policy

1. Introduction

1.1. Background to the study

Cybersecurity threats have seen an exponential rise since the start of the COVID-19 pandemic and have created many issues for organisations (Pranggono & Arabo, 2021). Cybercriminals have used phishing and malware attacks as their preferred mode of attacks (Eian et al., 2020; Lallie et al., 2020; Minnaar, 2020). Cyberattacks have been widely reported in South Africa, where cybercriminals have exploited factors, such as, work from home and the reliance on technology (Mabuza, 2020; Naik, 2021).

The rise in working from home has shifted the predominant source of cybercrime to the insider; these are individuals that work for organisations, including those who work from home. Cybercriminals have been found to exploit COVID-19 pandemic-induced contextual factors (referred to hereafter as COVID-19 factors) to carry out their nefarious actions with a significant level of success (Naidoo, 2020). These factors have an impact on the compliance behaviour of telecommuting employees in organisations with information security policies. However, current measures have not been enough to effectively stop cybersecurity incidents.

The COVID-19 pandemic has had an impact on the organisational context, for example telecommuting has become the norm and this has affected information security governance. Organisations need to strengthen security measures by updating information security policies, adjusting relevant security measures, and prioritising information security awareness of employees since the reliance on technology has left organisations vulnerable to cyberattacks (Eian et al., 2020).

A limited number of studies have been conducted on the impact in the South African context of the COVID-19 pandemic on employee compliance behaviour and changes in information security governance. The increase in cyberattacks during the pandemic and its potential long-term consequences on information security highlight the need for research in this area. The COVID-19 pandemic has significantly impacted people's lifestyles and work patterns, leading to notable implications for cybersecurity (Barnes, 2020).

1.2. Research problem

There has been a major upsurge in cybersecurity attacks since the start of the COVID-19 pandemic (Pranggono & Arabo, 2021); with the rise in telecommuting, cybercriminals have identified a new frontier, posing a significant challenge for organisations. Telecommuting employees must generally rely on their awareness of security threats and on their confidence in their ability (self-efficacy) to counter them (Michaelides, 2021; Taghva, 2021b). COVID-19 pandemic-induced factors that impact on individuals, such as fear, compromised mental health, information overload, and a risk of unemployment, may influence their information security behaviour. Hence, organisations need to review their security policies and this shift in information security governance is essential for the survival of organisations.

Factors influencing the adaptation of security policies can be categorised as organisational, human, and technological (Werlinger et al., 2009). An understanding of COVID-19 pandemic-induced contextual factors underlies the reasons for organisations to update existing security policies or to adopt new information security policies. Existing security standards need additional provisions

catering for telecommuting (Scarfone et al., 2020). Adapting existing information security policies is essential for organisations seeking to address the 'new normal' of telecommuting and other COVID-19 pandemic-induced contextual factors.

1.3. Research goal

This study explained how COVID-19 pandemic-induced contextual factors influenced the compliance behaviours of employees in organisations in South Africa. This study also explored how telecommuting influenced security policies, the procedures of organisations and compliance behaviour, and how security policies and procedures brought in since the pandemic have influenced compliance behaviour. In the next section, the research question will be posed.

1.4. Research question

1. How do COVID-19 pandemic-induced contextual factors influence information security compliance behaviour among employees?

Sub-research questions

1. How does telecommuting resulting from the COVID-19 pandemic influence the security policies and procedures of organisations?
2. How do organisational security policies and procedures motivate compliance behaviour of employees?

1.5. Research objective

The main objective is:
To determine how COVID-19 pandemic-induced contextual factors impact the information security policy compliance behaviours of employees.

Sub-research objectives

1. To determine how telecommuting influences security policies and procedures of organisations.
2. To determine how organisational security policies and procedures influence the compliance behaviour of employees to security policies.

1.6. Significance of the research

The COVID-19 pandemic has had a significant impact on cybersecurity globally (Minnaar, 2020) and cybercriminals have exploited COVID-19 pandemic-induced contextual factors. There is a need to understand how the COVID-19 pandemic has influenced information security policy compliance and information security governance regarding the adaptation of security policies, especially in the African context.

This study will help organisations understand how the COVID-19 pandemic has impacted on information security. This will guide information security policy and practice in organisations. Researchers will benefit from the proposed study; the body of knowledge on the impact of COVID-19 pandemic-induced contextual factors on organisations globally and more so in the African context is limited. Findings in this study will present researchers with a greater understanding of the impact of COVID-19 pandemic-induced contextual factors on compliance and information security governance. This study will help grow the body of knowledge on this relevant topic.

1.7. Structure of dissertation

The dissertation is structured as follows:

Chapter 2: A review of literature is presented in the section. Justification of the concepts and theories relevant to the dissertation are discussed in detail.

Chapter 3: Discusses the theoretical background to the study giving an in depth understanding of key concepts adopted.

Chapter 4: The methodological approaches and methodologies adopted are discussed.

Chapter 5: The analysis of the collected data is discussed, and the findings are presented.

Chapter 6: Ends with the recommendations, a discussion of the findings and the conclusion.

2. Literature review

This literature review delves into studies on compliance behaviour, information security governance, and COVID-19 pandemic-induced contextual factors to understand how these areas are related and to help develop the conceptual framework for the study.

Section 2.1 analyses studies that have been conducted on compliance behaviour to understand factors in compliance behaviour, the standard theories, methodologies, and contexts of studies on compliance. In Section 2.2, information security governance is explored; this section looks at what is known about information security governance, how the knowledge about security governance impacts on compliance, and how COVID-19 pandemic-induced contextual factors are correlated with security governance. Finally, in Section 2.3, the COVID-19 pandemic-induced contextual factors are discussed.

2.1. Compliance

Information security policy is one of the most effective security measures. Technological security measures such as anti-malware tools and firewalls are simply not enough to prevent cyberattacks (Alsmadi et al., 2018). Having employees that comply with security policies shows a robust information security culture which is an essential prerequisite for strong information security (Price, 2014; Siponen et al., 2009; Solomon & Brown, 2021).

Compliance is a problem facing organisations everywhere; previous studies have looked at how protective measures, subjective norms and deterrence measures motivate compliance behaviour. Due to the high number of cyberattacks since the pandemic, researchers and industry experts argue that pandemic-induced contextual factors have influenced compliance behaviour (Coles-Kemp & Theoharidou, 2010; Warkentin & Willison, 2017). This makes the problem of compliance very important and one that requires exploring.

This section examines findings of salient studies specifically on compliance behaviour to understand which factors have been identified as influencing compliance behaviour (see Table 1 to Table 5).

2.1.1. Information security behaviour

Information security deals with the confidentiality, integrity, and availability of information systems (Stanton et al., 2004). Information security behaviour is any behaviour that has implications for information security; compliance behaviour is considered an essential facet of information security behaviour and information security management (Box & Pottas, 2013; Warkentin & Johnston, 2008). Compliance to security programs is typically associated with good information security behaviour (Hamid et al., 2017).

2.1.2. Factors influencing compliance

Numerous factors have an impact on the compliance behaviour of employees (see Table 1). Compliance behaviour is a broad area of study with many implications. Organisational factors have an impact on the compliance behaviour of employees (Alshare et al., 2018; Dong et al., 2021; Solomon & Brown, 2021) and cover various areas, some of which have not been explored in the African context and related to the COVID-19 pandemic.

Table 1. Factors influencing compliance behaviour

Author(s)	Factor(s)
Jeon et al., 2020	Work impediments, perceived responsibility, and self-efficacy
Liu et al., 2021	Punishment expectancy
Nasirpouri Shadbad & Biros, 2020a	Technostress resulting from IT use
Kim & Han, 2018	Corporate social responsibility
Alshare et al., 2018	Procedural justice, distributive justice, severity and swiftness of sanction, privacy, responsibility, and organisational security culture
Aurigemma & Mattson, 2017	Sanctions
Karlsson et al., 2017	Employees' intentions to comply, self-efficacy and awareness of information security policies
Kim & Kim, 2017	Compliance intention belief and social pressure
Li et al., 2019b	Continuity and mandatory demands
Li et al., 2017	Technical quality, perceived reasonableness, and perceived convenience
Iriqat et al., 2019	Deterrence and protection motivations
Yazdanmehr et al., 2020	Social influence at both individual and organisational levels
Addae et al., 2019	Perceived threat, vulnerability, response cost, and efficiency
Hooper & Blunt, 2019	Self-efficacy; and perceived impact of a potential event; with cues to action exerting a significant influence on that perceived impact
Safa et al., 2016	Information security knowledge sharing, collaboration, intervention and experience
Solomon & Brown, 2021	Organisational culture and information security culture.
Wiafe et al., 2020	Attitude towards information security compliance mediates the effects of personal norms on compliance intention.

2.1.3. Most commonly used theories in recent compliance studies

The commonly used theories used in studies on compliance behaviour are derived from protection motivation theory, theory of planned behaviour and the general deterrence theory (Nasir et al., 2018) (see Table 2). Few studies have been conducted using contextual factors related to COVID-19, this is primarily because COVID-19 is a novel phenomenon; the manner in which COVID-19 appeared and how it changed how people live their lives overnight has created many opportunities for researchers.

Table 2. Common theories in compliance studies

Theories utilised	Studies
Protection motivation theory	Addae et al., 2019; Hooper & Blunt, 2019; Iriqat et al., 2019; Jeon et al., 2020; Karlsson et al., 2017; Mwagwabi & Jiow, 2021
Theory of planned behaviour	Kim & Kim, 2017; Li et al., 2017; Wiafe et al., 2020
General deterrence theory	Alshare et al., 2018; Aurigemma & Mattson, 2017; Hooper & Blunt, 2019; Iriqat et al., 2019
Organisational culture and information security culture	Solomon & Brown, 2021

Theories utilised	Studies
Self-efficacy, perceived responsibility, work impediment and autonomy model	Jeon et al., 2020
Compliance theory	Liu et al., 2021
Control theory	Liu et al., 2021
Descriptive norms	Wiafe et al., 2020
Personal norms	Wiafe et al., 2020
Neutralization theory	Alshare et al., 2018
Justice theory	Alshare et al., 2018
Technostress	Nasirpouri Shadbad & Biros, 2020a
Rational choice theory	Kim & Han, 2018
Corporate social responsibility	Kim & Han, 2018
Value-monistic	Karlsson et al., 2017
Security awareness	Karlsson et al., 2017
JD-R model	Li et al., 2019b
Psychological resource theories	Li et al., 2019b
Social contingency model	Yazdanmehr et al., 2020
Theory of reasoned action.	Hooper & Blunt, 2019
Social bonds theory	Safa et al., 2016
Normative beliefs	Mwagwabi & Jiow, 2021

2.2. Information security governance

Information security is an overarching category which deals with all aspects of information security policy management in an organisation (da Veiga & Eloff, 2007; Knapp et al., 2009). Information security governance facilitates the execution of security policies and procedures in organisations (Warkentin & Johnston, 2006). Information security governance is vital in ensuring that appropriate security measures are in place to mitigate cybersecurity threats. The adoption of information security governance is typically undertaken by the board and management of organisations (Posthumus & von Solms, 2004; von Solms & von Solms, 2006).

An information security culture is where everyone works together to protect their organisation from threats; this is hardly possible without effective information security governance (AlGhamdi et al., 2020; da Veiga & Eloff, 2007; Koh et al., 2005). Information security governance deals with all the aspects which result in a cohesive information security culture, where employees are aware of information security policies and procedures and where these are enforced and routinely updated and monitored.

Information security governance is dependent on external and internal factors; often awareness of threats from sources external to the organisation are why that organisation has introduced information security governance to some extent (Knapp et al., 2009). Internally, organisational culture influences the compliance behaviour of employees in the workplace (Solomon and Brown,

2021). Organisations with adequate information security governance are unlikely to have many cases of noncompliance (Alshare et al. 2018).

Several studies on compliance behaviours have recognised that organisational factors have an impact on compliance behaviour and used this knowledge in their information security governance recommendations (Schinagl & Shahim, 2020; Williams et al., 2013). However, more studies on compliance behaviour are needed that focus on organisational factors (Angraini et al., 2019).

Cybersecurity threats have been reported worldwide since the start of the COVID-19 pandemic. However, the biggest and most significant organisational change resulting from the pandemic has been working from home (Jasgur, 2021). At the same time employees working from home have become insider threats (Chapman, 2021). This has resulted in the need for organisations to review security policies and make necessary adaptations to fit the "new normal". Figure 1 illustrates a proposed model for governance processes.

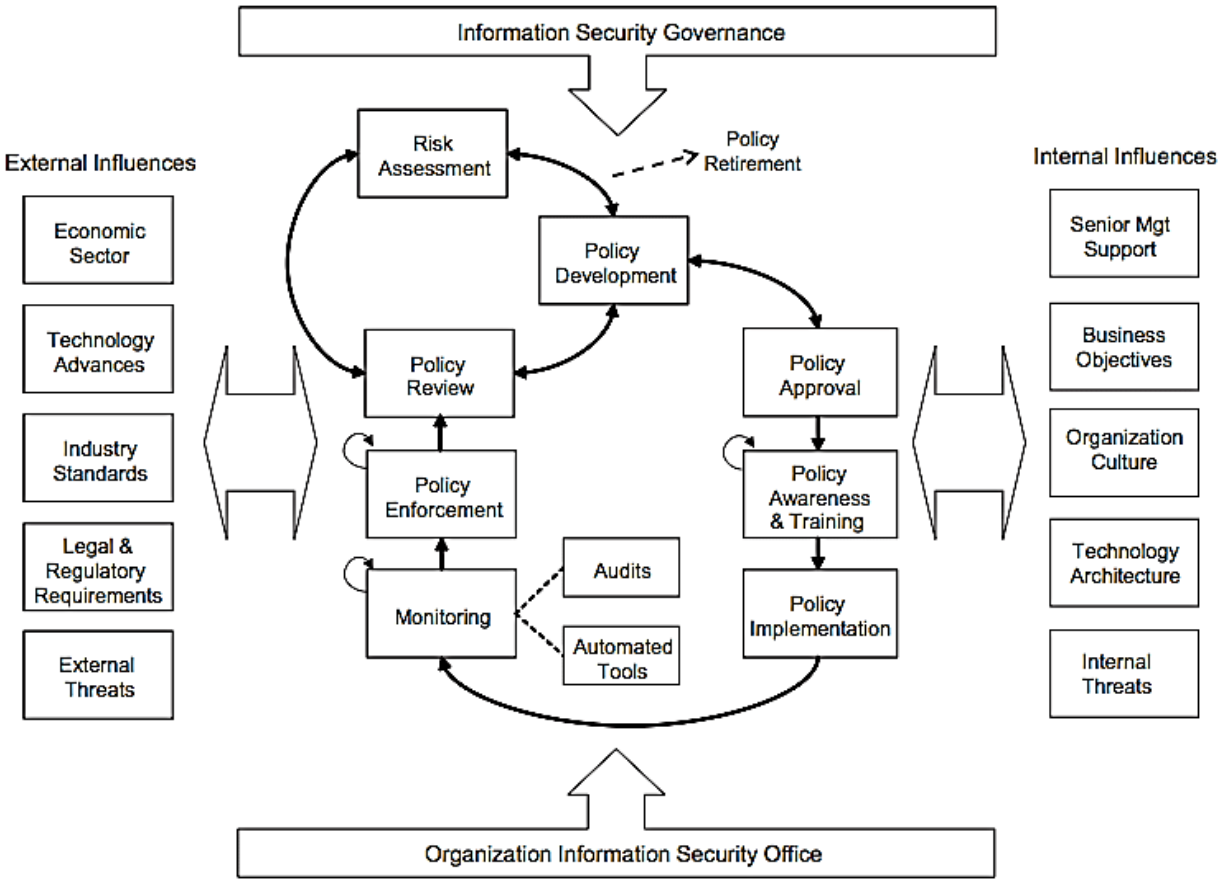

Figure 1. An organisational-level process model (Knapp et al., 2009).

A core component of the information security governance model (see Figure 1) is policy development, and this can also help organisations confront the new cybersecurity threats encountered since the pandemic. Policy development is essential in instances where organisations have no existing information security policy and where a review of information security policies is necessary (Singh & Gupta, 2013; Williams, 2001). Security policy review procedures include ensuring that amendments to existing policies are implemented.

In the following subsections, this literature review will look at security policy reviews, policy awareness and the internal threats in the context of employees who work remotely. The organisational-level information security governance process model (Knapp et al., 2009) will be used explain information security governance in the context of telecommuting (see Figure 1). The information security governance process identifies policy review, policy awareness, internal threats, and external threats as key elements of the organisational information security governance process.

2.2.1. Policy review

In organisations that already have security policies, ensuring that they are regularly monitored, updated, maintained, and adjusted according to new threats is vital for effective information security governance (Flowerday & Tuyikeze, 2016; Höne & Eloff, 2002; Knapp et al., 2009). These actions are associated with policy review processes (Knapp & Ferrante, 2012a). The pandemic-induced transition to working from home made it necessary for organisations to review information security policies (Aljohani, 2021). However, this may not have been required for organisations that already had security policies that covered aspects of telecommuting.

A recent study conducted in the United Kingdom found that only 32% of organisations with security policies covered the remote work aspect (Renaud & Ophoff, 2021) and this shows that there have been shortfalls in the governance of working from home. Another study, also conducted in the UK, found that 75% of organisations in the UK did not have cybersecurity-related rules for staff to follow when working from home (Furnell & Shah, 2020). However, telecommuting employees need to maintain an information security culture even under changed circumstances and this can only be accomplished by developing and enforcing necessary information security policies (Furnell & Shah, 2020).

It's essential for employees working from home to feel that their own data is safe in the face of cybersecurity threats. Information security policies and guidelines for telecommuting not only protect organisations but the private data belonging to the employee as well (Jasgur, 2021; Sturgeon, 1996). Security policies give employees peace of mind when conducting their tasks using organisation resources; without clear guidelines, it may be difficult for them to know what rules exist. During the COVID-19 pandemic it became important for employees to be aware of what they should and should not do when working from home (Brown & Capstone, 2020). It is, therefore, essential for organisations without security policies for telecommuting to establish necessary policies for this new reality.

A study which was conducted to understand the pandemic's impact on the cybersecurity policies of a European organisation explains that the COVID-19 pandemic brought changes that have not been experienced before (Carrapico & Farrand, 2020). Working from home is highlighted as an important consideration in this developing a cybersecurity strategy (de Schrijver & van Loon, 2021).

The COVID-19 pandemic has resulted in organisations needing to seek ways to manage the potential risks of telecommuting (Abukari & Bankas, 2020). Telecommuting employees are at risk of allowing an organisation to become vulnerable to cybersecurity threats because of the perceived lack of support, isolation, and related COVID-19 pandemic-induced contextual factors that such employees experience (Okereafor, 2020). The pandemic has had an impact on how employees in organisations work. Telecommuting has become the norm since the start of the COVID-19 pandemic (Lee & Han,

2021); therefore, organisations have had to accept this reality and review and update measures for this where these are absent.

2.2.2. Policy awareness

Employees' awareness of security policies is a crucial part of information security governance. The governance process model in Figure 1 indicates that before and repeatedly while implementing and enforcing adopted or adapted information security policies, it is essential to make employees aware of these policies (Knapp et al., 2009).

Since the start of the COVID-19 pandemic it has become necessary for organisations to make employees aware of existing information security policies which address common cybersecurity threats targeting employees who have to work from home (Crossland et al., 2021). Awareness campaigns related to cybersecurity impact on the information security policy behaviour of employees (Li et al., 2019a). Recognition of this impact provides an impetus for awareness programs regarding security policies and all aspects of cybersecurity in organisations, no matter where employees find themselves working.

2.2.3. Insider threats

An insider threat comes from someone, often an employee, who has access to the resources of an organisation; these individuals may deliberately abuse their access to commit cybercrime or may unwittingly fall victim to cybercrime and as part of this compromise the organisation’s information resources (Dupuis & Khadeer, 2016; Greitzer et al., 2008).

Telecommuting has exacerbated the insider threat as often telecommuting employees are not monitored (Chapman, 2021). Various contextual factors may make it difficult for employees to follow security policies and procedures effectively and hence leave employees who are working from home vulnerable. It is therefore important for individuals working from to receive help to maintain the necessary level of information security (Borkovich & Skovira, 2020a; Okereafor & Manny, 2020).

However, there are also other COVID-19 pandemic-induced contextual factors that have worsened the insider threat. These include job insecurity that has impact on the commitment, job satisfaction and the features of the new workplace such as noise or interruptions that negatively affect the productivity of employees (Omar, 2015; Al-Tabash & Happa, 2018). These all potentially compromise organisations in terms of expected compliance to set information security policies.

2.2.4. External threats

An external threat is a threat that is external to the organisation or institution (Zadig & Tejay, 2010). During the COVID-19 pandemic, external threats exacerbated the insider threat to significant effect. Perhaps the most used attack vector used by external threats is phishing (Arduin, 2020). This form of attack is highly dependent on internal factors as it requires the attacker to interact with the insider, resulting in a malware attack (Mell et al., 2005). External cybersecurity threats have been found to have benefitted from contextual factors associated with the pandemic as many external threats were facilitated by the lack of employee productivity as well as the lack of satisfaction regarding the workplace.

2.3. COVID-19 pandemic-induced contextual factors

Studies conducted on the impact of contextual factors on policy have had limitations in that they looked only at contextual factors drawn from well-established behavioural theories such as deterrence theory and the protection motivation theory (Johnston et al., 2017; Mcbride et al., 2012). The study by Johnson et al. (2017) suggests more studies that focus specifically on contextual factors are required; this creates an avenue for future work.

The COVID-19 pandemic has been recognised as having had an impact on information security (Carroll & Conboy, 2020; Lueck, 2020). In addition, COVID-19 pandemic-induced contextual factors have been noted in the literature as being drivers of cybersecurity incidents. However, no quantitative study has been found that explains how all the identified factors influence compliance behaviour. This section will discuss the telecommuting norm, information overload, job insecurity, technostress, and the fear as relevant factors.

2.3.1. Telecommuting norm

The most significant and abrupt change resulting from the pandemic has been the adoption of telecommuting arrangements in organisations. Due to stay-at-home orders, people were required to work from home; for many working people it meant telecommuting was established as a norm (Collins et al., 2020; Holliss, 2021). Norms are an event or act which is accepted as usual; thus, the telecommuting norm is defined as the adoption of telecommuting in organisations. Because of how abrupt it was and because many organisations were unprepared, telecommuting created ripple effects in organisations' information security.

Telecommuting not only impacted the information security governance of organisations with regards to security policies and procedures in organisations, but it also bred more cybersecurity threats as often employees working remotely were isolated without any supervision and unaware of cybersecurity threats exploiting the new normal (Agbodzie, 2020; Borkovich & Skovira, 2020b) (see Table 3 for other negative factors associated with telecommuting). Additional factors related to further undermine employees' information security practice.

Table 3. Negative impact of work-from-home arrangements

Harmful remote work-related factors	**Source(s)**
Burnout and related stress	Golden et al., 2008; Samek Lodovici, 2021
Prolonged isolation	Golden et al., 2008; Samek Lodovici, 2021
Unreliable internet connection	Lewis, 2013; Samek Lodovici, 2021
Work-life conflict	Samek Lodovici, 2021
Limited digital skills	Samek Lodovici, 2021
A lack of supervision	Golden et al., 2008; Samek Lodovici, 2021

Several studies, mostly prior to the COVID-19 pandemic, have been conducted to understand the role of telecommuting in organisations (Gerard & Caillier, 2012; Hunton & Norman, 2010; Nyaanga, 2012; Onder, 2016; Wang et al., 2020), but organisational studies related to information security governance and telecommuting are few.

Telecommuting intensity is defined as the length of time that employees work remotely (Spilker, 2014); the hybrid work arrangement where workers go into the office on certain days or for a particular meeting has made telecommuting intensity a pertinent subject since the pandemic. Treating telecommuting as a single theme with generalisable outcomes tends to overlook the variations in intensity of work-from-home arrangements in the workplace; the intensity of telecommuting can have significant implications for employees (Gajendran & Harrison, 2007).

Although there has been an increase in the study of telecommuting intensity since the pandemic, very few studies have been conducted to understand telecommuting intensity and its impact on compliance behaviour.

2.3.2. Information overload

Information overload is defined as an overabundance of information on specific subjects. This may result in individuals not making the right decisions based on how difficult it may be to assimilate and comprehend all this information (Borkovich, 2018). The concept of information overload has generated several similes and associated terms many of which are new words; these include information overabundance, infobesity, infoglut, data smog, information pollution, information fatigue, social media fatigue, social media overload, information anxiety, library anxiety, infostress, infoxication, reading overload, communication overload, cognitive overload, information violence, and information assault (Bawden & Robinson, 2021).

Information overload is a umbrella term and has become prominent in many studies related to the COVID-19 pandemic (Bermes, 2021; de Bruin et al., 2021; Mladenović et al., 2022). An interesting finding is that, as a result of work-from-home arrangements, employees have had to learn to tolerate an increased amount of information, some which is not related to work (Schmitt et al., 2021; Wang et al., 2022). Furthermore, it has been noticed that the pandemic, technostress, and information overload have become related phenomena (Ghislieri et al., 2021). Hence, studies have shown firstly that information overload has impact on the stress levels and well-being of individuals (Fan & Smith, 2021; Mohammed et al., 2022) and secondly information overload has an impact on information security related behaviours of employees (Desolda et al., 2021).

2.3.3. Technostress

Technostress is the stress individuals experience because of exposure to new technologies (Ragu-Nathan, Tarafdar, Nathan, et al., 2008). Telecommuting necessitates the adoption of software and associated technologies and hence there has been a need for employees to use virtual private networks, cloud computing and business communication tools even from their home office (De' et al., 2020). Unfortunately, it is highly possible that many employees were not familiar with these applications before the pandemic.

Six subtypes of technostress are identified in literature, namely techno-overload, techno-complexity, techno-uncertainty, techno-invasion, techno-unreliability, and techno-insecurity (Nasirpouri Shadbad & Biros, 2020a). Hence, technostress (see Table 4) covers a wide array of technical stressors.

The pandemic has worsened technostress in the workplace. Studies indicate that technostress has a level of impact on employees similar to other types of stress (Kot, 2022; Stana & Nicolajsen, 2021). Technical stressors have varying impacts on employees' behaviours no matter where the workplace

is located and this has made technostress a pertinent issue for employees who are working from home (Harris et al., 2022; Ingusci et al., 2021; Spiess et al., 2021).

Table 4. Types of technical stressors

Techno-stressors	Description
Techno-overload	Relates to situations where employees feel that the information they are receiving is challenging to manage, complicated and difficult to process (Brivio et al., 2018).
Techno-complexity	Describes situations where employees feel that technologies are too difficult to understand (Brivio et al., 2018).
Techno-uncertainty	Describes situations where information technologies constantly change, thus disturbing users and creating uncertainty about learning new systems (Ragu-Nathan, Tarafdar, Ragu-Nathan, et al., 2008).
Techno-invasion	Describes situations where employees feel that they should always be connected and available to work requests (Brivio et al., 2018; Ragu-Nathan, Tarafdar, Ragu-Nathan, et al., 2008).
Techno-unreliability	Describes situations where information technologies are unavailable or do not work as they should (Fischer et al., 2019).
Techno-insecurity	Relates to employees feeling insecure about losing jobs because of their inability to adapt to changes in systems or because they lack digital skills (Ragu-Nathan, Tarafdar, Ragu-Nathan, et al., 2008).

It is important to understand the impact of technostress in the context of cybersecurity. While a study by Nasirpouri, Shadbad and Biros (2020a) looked at technostress and its impact on the behaviour of employees in relation to information security in the research reported on in this dissertation it was considered that it was important to study many potentially relevant technical stressors in different contexts.

2.3.4. Fear

The pandemic aroused a lot of fear globally; fear is defined as an unpleasant emotional state which is triggered by the perception of negative stimuli (Hoog et al., 2008). People were not only fearful of contracting a lethal virus but were also fearful of losing their livelihoods (see Table 5 for factors associated with fear of COVID-19). Fear has been included in research to explain the deviant information security behaviour of employees in organisations (Xu et al., 2017). Furthermore, fear has previously been measured in quantitative studies to determine its impact on the intention of employees to comply with security programs (Hassandoust & Techatassanasoontorn, 2020). However, fear factors associated with the pandemic was not explored in that study.

Fear is related to uncertainty (Tiedens & Linton, 1994) (for example, an uncertain business environment). A recent study on uncertainty related to the pandemic could not establish the impact of uncertainty on information security behaviour (Kautondokwa et al., 2021). However, in that study the job insecurity that impacted many globally due to the COVID-19 pandemic was not explored.

Table 5. Fears associated with the COVID-19 pandemic

Fears observed since the pandemic	Source(s)
Impact on personal economy	Binder, 2020; Mertens et al., 2020
Health implications	Binder, 2020; Mertens et al., 2020
Fatality of virus	Mertens et al., 2020
Quarantine	Mertens et al., 2020
Fear of infection	Asmundson & Taylor, 2020; Binder, 2020
Impact on the economy	Binder, 2020; Mertens et al., 2020
Collapse of the healthcare system	Asmundson & Taylor, 2020; Mertens et al., 2020

Cybercriminals have used various attack vectors to target vulnerable individuals, mainly using electronic communications methods to contact victims and leveraging the fear that many individuals harbour since the pandemic. Messages from cybercriminals often included content related to the pandemic, such as health-related communications and communications related to the jobs of employees. These strategies have left individuals susceptible to attacks (Fontanilla, 2021; Meilee et al., 2020). There has also been a focus on fear for the safety of others since the pandemic, in the next section, altruistic fear will be briefly explored.

Altruistic fear

Altruism is defined as attributes related to the welfare of others (Warr & Ellison, 2000a). Several studies related to information security and Information Systems explored the role of altruistic traits on the behaviour of individuals (Ichimura et al., 2017; Lee & Lee, 2010; Youn et al., 2021) and recent studies have looked at the impact of altruistic fears (fear for the safety of others related to the COVID-19 pandemic) on individual behaviours (Sloan et al., 2021). However, no studies were found that explored the role of altruistic fear on the information security policy compliance of employees or as a moderator in the relationship between job insecurity and compliance.

2.3.5. Job insecurity

Job insecurity is an individual's perception of powerlessness due to a threatening work situation (Greenhalgh & Rosenblatt, 1984). Millions lost jobs as a result of the COVID-19 pandemic, and the pandemic threatened the working conditions of many as organisations looked for ways to cut costs (Wilson et al., 2020). Job insecurity is considered to be a work stressor (de Witte, 2010; Meltzer et al., 2009) and it adversely affects the attitudes of employees towards their tasks (Smit et al., 2016). This insecurity, uncertainty and fear created problems for the information security of organisations as cybercriminals capitalised on job insecurity (Kantor, 2021; Monroe, 2020).

2.4. Summary

The COVID-19 pandemic had an impact on organisations globally and pandemic-induced contextual factors also had an impact on the overall compliance behaviour of employees. It is predicted that the impact of the pandemic on organisations will be felt for many years to come.

Numerous factors influence compliance behaviour. Previous studies have looked at factors that influence compliance behaviour using the protection motivation theory, theory of planned behaviour,

and deterrence theories. Very few studies have been conducted to understand the impact that the pandemic-induced contextual factors have had on compliance behaviour; this has created a gap in research.
Organisations had to act after stay-at-home orders were instated during the pandemic. However, employees were expected to still work during the pandemic and to be productive; necessary measures were required to make this possible and safe for organisations and employees taking into account the cybersecurity threats that were present and were leveraging on the vulnerabilities of many due to the pandemic.

COVID-19 pandemic-induced contextual factors impacted the security policies and procedures of organisations, as witnessed by the changes that many organisations had to make during the pandemic. However, few academic research studies have been conducted to understand compliance behaviour as it relates to the contextual factors and the impact this had on the security policies and procedures of organisations. COVID-19 and other infectious diseases are expected to persist for many years and the new norm is likely to become established and to persist even after the pandemic ends. Hence, COVID-19 pandemic-induced contextual factors will continue to impact cybersecurity.

The hypotheses will be presented in the next section,

3. Theoretical background

The constructs adopted in the conceptual model (Figure 2) were drawn from theories in the literature. This section will present the hypotheses and will scrutinise the adopted conceptual model. A summary of the hypotheses adopted in this study a presented in Table 6. The theoretical background of this study follows.

3.1. COVID-19 pandemic-induced contextual factors

For organisations without policies regulating work-from-home arrangements a review of policies need to be initiated, and for organisations with policies that make provision for telecommuting, security policy awareness and more security measures are a priority (Murphy, 2020; Radzikowski, 2020; Richberg, 2020). It is predicted that aspects of information security governance in organisations will be viewed positively as being a result of telecommuting as this shows a level of proactivity from the side of organisations. Therefore, the following is hypotheses are proposed:

Hypothesis 1: Telecommuting norm has a positive impact on the policy awareness programmes of organisations.
Hypothesis 2: Telecommuting norm has a positive impact on the policy review programmes of organisations.

Telecommuting intensity, or the amount of time employees work from home, has a negative impact on the work life balance of employees (Alfanza, 2021). Furthermore, telecommuting intensity will have a negative impact on the behaviour of employees as poor work life balance contributes to stress and a perceived feeling of overload of employees (Byrne, 2005; Poulose & Dhal, 2020) and this in turn may negatively affect compliance behaviour. Therefore, this study proposes the following hypotheses:

Hypothesis 3: Telecommuting intensity positively moderates the relationship between information overload and compliance behaviour, such that information overload has a more substantial negative impact on the compliance behaviour of employees with higher levels of telecommuting intensity compared with those with lower levels of telecommuting intensity.

Hypothesis 4: Telecommuting intensity positively moderates the relationship between technostress and compliance behaviour, such that technostress has a more substantial negative impact on the compliance behaviour of employees with higher levels of telecommuting intensity compared with those with lower levels of telecommuting intensity.

Information overload has a negative impact on telecommuting employees (Åborg & Fernström, 2002; Fonner & Roloff, 2010); this may be because employees who are working from home have to handle a lot of information that they receive by electronic mail and via business communications platforms and this may be difficult for employees to process (Vasic, 2020).

The research findings of Segal (2021) showed that 38% of employees believed that information overload is likely to push them to quit their jobs, 89% of employees thought that business communication tools such as MS Teams are exhausting. These findings demonstrated the impact of information overload on employees.

Information overload has an impact on the stress levels of individuals and their mental health (Hu & Chen, 2011; Mungly et al., 2012). These factors leave employees vulnerable to cyberattacks as they are likely to impair information security behaviour especially during the pandemic. Thus, the following hypothesis is proposed:

Hypothesis 5: Information overload has a negative impact on the compliance behaviour of employees to security policies.

Technostress has a negative impact on the compliance behaviour of individuals (Hwang & Cha, 2018; Nasirpouri Shadbad & Biros, 2020b). Technostress is associated with the adoption of information communication technologies (ICTs) and an increase in technostress has an impact on the compliance behaviour of individuals, so the following hypothesis is proposed:

Hypothesis 6: Technostress has a negative impact on the compliance behaviour of employees to security policies.

When employees are unhappy due to factors such as job insecurity, they may not be compliant with information security policies (Lang et al., 2016). However, this is not the only threat that faces organisations, job insecurity has exacerbated the insider threat as unhappy employees are increasingly likely to misuse confidential information (Brands, 2021; Crosman, 2020; Nurse et al., 2021). The following hypothesis is proposed:

Hypothesis 7: Job insecurity has a negative impact on the compliance behaviour of employees to security policies.

Rather than personal fear, altruistic fear has a significant impact on the behaviours of individuals (Drakulich, 2015; Warr & Ellison, 2000b). Studies focussing on the pandemic used fear in a moderating role between job insecurity and the health of employees, finding that fear and job insecurity have a level of negative impact on employees (Blanuša et al., 2021; Gasparro et al., 2020). No study was found looking at the compliance behaviour of employees, however, since compliance behaviour is generally related to human behaviour which has been shown to be impacted by fear, the following hypothesis is proposed:

Hypothesis 8: Altruistic fear of the coronavirus positively moderates the relationship between job insecurity and compliance behaviour, such that job insecurity has a substantially stronger negative impact on the compliance behaviour of employees with high levels of Altruistic fear of the coronavirus compared with those with lower levels of Altruistic fear of the coronavirus.

3.2. Information security governance

The two essential aspects in information security governance are information security policy awareness and information security policy reviews. The security awareness of employees who are working from home as a result of the pandemic has had an impact on their adherence to security policies and procedures in their organisations (Taghva, 2021a). Therefore, security policy awareness should be prioritised amongst employees required to work from home. These employees are relatively aware of what is required of them to protect themselves from cybersecurity threats.

Nevertheless, it is suggested that awareness and training be prioritised as threats evolve (Georgiadou et al., 2021).

Managing information security policies in the workplace will result in information security in an organisation (Knapp & Ferrante, 2012a). The following hypotheses are thus proposed:

Hypothesis 9a: Information security policy awareness has a positive impact on the compliance behaviour of employees.
Hypothesis 9b: Information security policy reviews have a positive impact on the compliance behaviour of employees.

Table 6. Summary of the adopted hypotheses for the study

Construct	Hypothesis	Definition
Telecommuting norm	Hypothesis 1	Telecommuting norm has a positive impact on the policy awareness programmes of organisations.
	Hypothesis 2	Telecommuting norm has a positive impact on the policy review programmes of organisations.
Telecommuting intensity	Hypothesis 3	Telecommuting intensity positively moderates the relationship between information overload and compliance behaviour, such that information overload has a more substantial negative impact on the compliance behaviour of employees with high levels of telecommuting intensity compared with those with lower levels of telecommuting intensity.
	Hypothesis 4	Telecommuting intensity positively moderates the relationship between technostress and compliance behaviour, such that technostress has a more substantial negative impact on the compliance behaviour of employees with high levels of telecommuting intensity compared with those with lower levels of telecommuting intensity.
Information overload	Hypothesis 5	Information overload has a negative impact on the compliance behaviour to security policies of employees.
Technostress	Hypothesis 6	Technostress has a negative impact on the compliance behaviour to security policies of employees.
Job insecurity	Hypothesis 7	Job insecurity has a negative impact on the compliance behaviour to security policies of employees.
Altruistic fear	Hypothesis 8	Altruistic fear of the coronavirus positively moderates the relationship between job insecurity and compliance behaviour, such that job insecurity has a substantially stronger negative impact on the compliance behaviour of employees with high levels of Altruistic fear of the coronavirus compared with those with lower levels of Altruistic fear of the coronavirus.
Policy awareness	Hypothesis 9a	Information security policy awareness has a positive impact on the compliance behaviour of employees.
Policy review	Hypothesis 9b	Information security policy reviews has a positive impact on the compliance behaviour of employees.

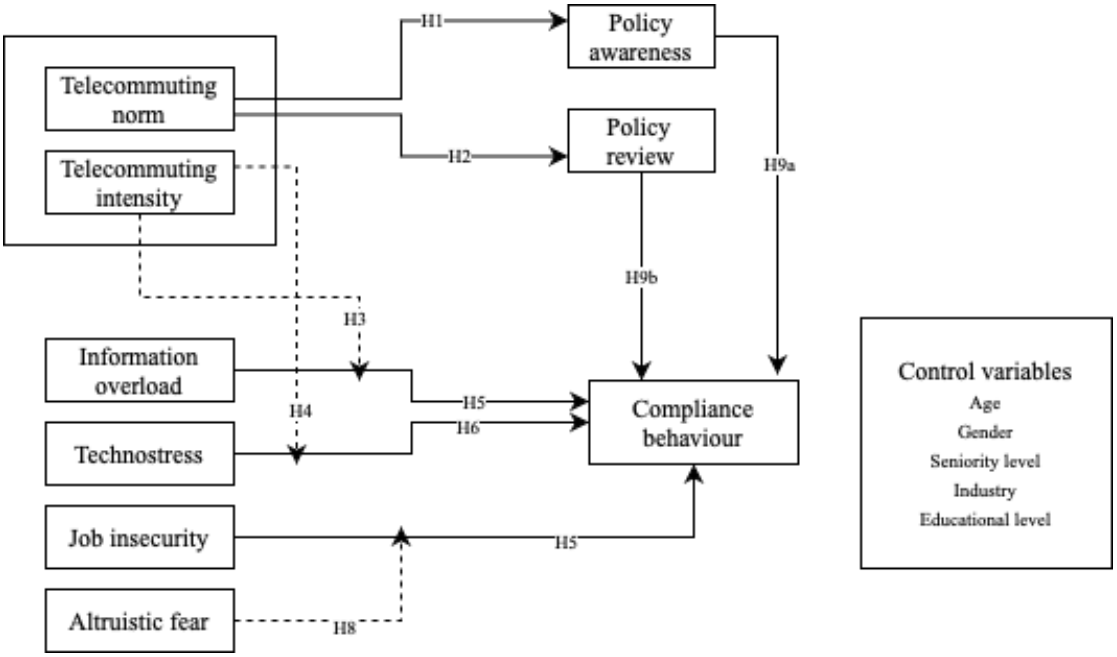

Figure 2. The conceptual model developed for the study.

The next section will look at the research methodology adopted.

4. Research methodology

4.1. Introduction

The research methodology highlights the required methods for collecting data (Bell & Waters, 2018). This research drew variables from previous studies for its conceptual model to investigate the research problem; the variables adopted for this study can be seen in Table 7. This section will discuss the link between the proposed conceptual framework and the design of the questionnaire.

The study, being deductive by nature, used statistical hypothesis testing to test the proposed hypotheses and to answer the research questions. Furthermore, the reliability and validity of the research outcome and the ethical considerations are discussed later in this section.

Table 7. Variables adopted in the study

Variable	Definition
Telecommuting norm	The act whereby organisations make it feasible for employees to work from home rather than working in the office (Handy & Mokhtarian, 1996).
Telecommuting intensity	Individuals who telecommute must replace the time they used to spend in the office with the time they spend working at home; the intensity is thus the amount of time individuals must work from home (Spilker, 2014).
Technostress	Technological advancements and the use of technology have impacted mental well-being, causing technostress (Ragu-Nathan, Tarafdar, Nathan, et al., 2008).
Information overload	With an abundance of information circulating on the news, social media and within organisations, it is said that too much information causes information overload (Borkovich, 2018).
Policy review	Organisational policy review procedures is how organisations monitor, maintain or update their information security policies (Knapp & Ferrante, 2012b).
Policy awareness	Organisation policy awareness deals with the policy awareness in organisations; is the level of awareness to information security best practices (Knapp & Ferrante, 2012b).
Altruistic fear	Fear in the context of the pandemic manifested itself as a result of the deadly nature of COVID-19, in the context of this study, altruistic fear is an individual's fear of what the virus would do to others (Anand & Chakravarty, 2020; Warr & Ellison, 2000a).
Job insecurity	With an increase in job losses, often employees are not sure about their job security which triggers job insecurity (Greenhalgh & Rosenblatt, 1984).
Compliance	The compliance of employees deals with the level that employees respond to their duties with regards to respecting information security policies (Safa et al., 2016).

4.1.1. Ontology

Ontology is a term concerning the nature of reality (Saunders et al., 2019). The ontological approach includes intersubjectivism, objectivism and subjectivism (Cunliffe, 2011; Holden & Lynch, 2006; Saunders et al., 2019). In objectivism, entities are independent of social actors, while in

intersubjectivism, reality is relative to the interactions between people in moments of time and space (Cunliffe, 2011). In subjectivism, social phenomena are created through the experiences of social actors (Saunders et al., 2019). The study approaches a reality independent of the researcher without the involvement of the participant's subjective experiences; therefore, as the researchers separate themselves from the objects being studied, objectivism is the adopted approach (Saunders et al., 2019).

4.1.2. Epistemology

Epistemology is a philosophical branch that studies the assumptions about knowledge (Saunders et al., 2019). The main epistemology approaches are positivism, critical realism, interpretivism, postmodernism and pragmatism (DeLuca et al., 2008; Saunders et al., 2019). Positivism and interpretivism are epistemologies often used in Information Systems studies (Kroeze, 2012). In the positivist approach, knowledge is in the form of facts and numbers, whilst in interpretivism, the researcher aims to include participants and their interpretation into some parts of a study (Saunders et al., 2019). The current study collected quantifiable data making positivism the appropriate approach.

4.1.3. Research approach

The approach to theory development is more than just the research philosophy, it directs the researcher as to the type of evidence to be collected, where and how it should be collected and how this evidence is interpreted (Saunders et al., 2019). The current study collected quantifiable data to be used to test hypotheses associated with compliance to information security policies during the COVID-19 pandemic. Essentially, the researchers separated themselves from the objects being studied. The deductive method is suitable in studies aiming to test hypotheses (this process can be seen in Figure 3) (Creswell, 2008; Saunders et al., 2019), thus this is the approach adopted.

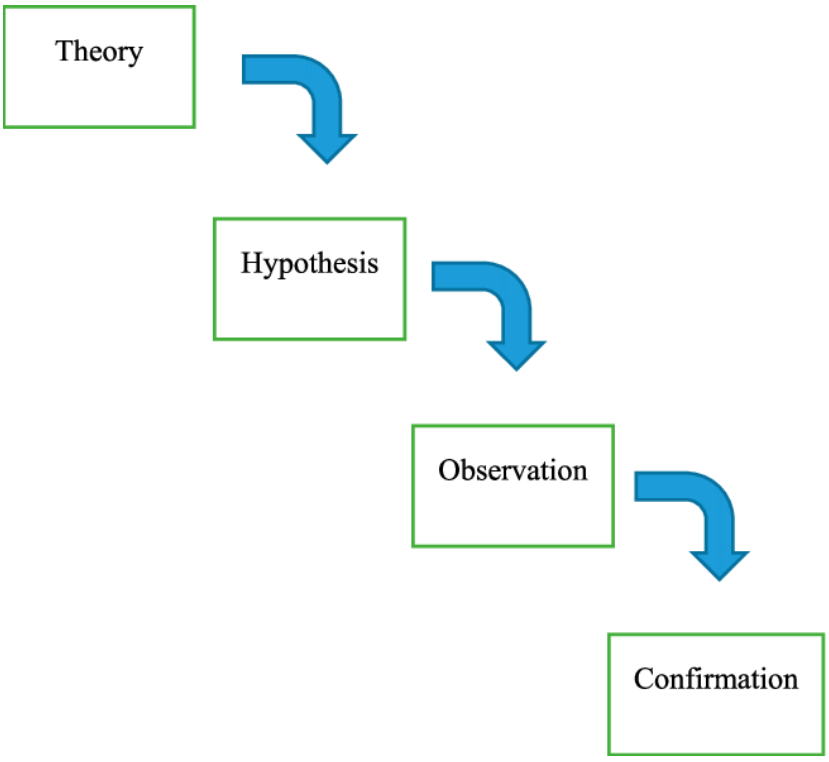

Figure 3. Deductive research stages (Turnbull et al., 2021).

It has been shown in the literature review that COVID-19 pandemic-induced contextual factors have been exploited by cybercriminals and subsequently have had an impact on the information security behaviour of individuals globally as has been observed through the exponentially high number of cybersecurity incidents and methods used in cybercrimes. The pandemic has also had a significant impact on the information security governance of organisations. A deductive method would be suitable for a study exploring these relationships further as this is likely to enable conclusions to be reached regarding the theoretically motivated propositions (Saunders et al., 2019). An inductive method would not be appropriate in a study of this nature as the proposed study does not start with a generalisation from an observation (Spielman et al., 2014) instead, it starts with a hypothesis, thus making inductive research inappropriate.

4.1.4. Research purpose

The purpose of the study is explanatory. This is because studies that conduct hypotheses testing explain the causal relationships of variables (Yegidis & Weinbach, 1991). This study developed hypotheses which were tested to enable causal deductions showing whether specific variables predict another (Yegidis & Weinbach, 1991).

4.1.5. Research choice

The study adopted a mono-methodological quantitative design suitable for studies using a survey questionnaire as the research instrument (Saunders & Tosey, 2013). The research instrument which was created posed questions to professionals working in organisations with security policies and operating in South Africa. Its purpose was to collect data that would assist the researchers to understand the influence of COVID-19 pandemic-induced contextual factors together with the organisation's security policies and procedures on the compliance behaviour of employees. The study adopted the quantitative methodology rather than the qualitative methodology because the explanatory nature of the study is to test specific hypotheses in order to understand a phenomenon (Stebbins, 2001).

4.1.6. Data collection

The study employed a survey questionnaire as the research instrument. Survey questionnaires are suitable in quantitative studies where the data is measurable (Creswell et al., 2007; deMarrais & Lapan, 2003). The questionnaire was distributed to a sufficient number of employees who work remotely and in organisations with information security policies using the Qualtrics software. This data would be used to assist the researcher to understand how COVID-19 pandemic-induced contextual factors and the information security governance in organisations impacted compliance behaviour. A seven-point Likert scale was used in the survey questionnaire, ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other with "Neither Agree nor Disagree" in the middle (Bertram, 2007). The Likert scale was adopted because it is effective in measuring attitudes and opinions, and it is generally recommended in quantitative Information Systems research.

4.1.7. Target population

The target population was employees working for organisations located in South Africa which have information security policies. The employees participating in this study were aware of the information security policies of the organisations for whom they work.

4.1.8. Sampling strategy

Sampling is important in gaining valuable information from the target population for research. Purposive sampling is a nonprobability sampling method that focusses on an identified subgroup in society; this method relies on the researcher's judgment when selecting the target units (Etikan et al., 2016). In the case of this study, Qualtrics Research Service identified a sample from employees in organisations with information security policies (Patton, 2002; Zack et al., 2019).

As a result of the pandemic, millions of South Africans had to work from home. Although a minimum number of ten respondents per item is considered acceptable when determining a suitable sample size (Hair et al., 2010), this study aimed to collect between 200 and 300 responses. Most studies on the compliance behaviour of individuals in society utilise a sample size between 200-300 (Sommestad et al., 2014). Furthermore, this sample size is suitable for a study of this nature although the method of data analysis, Partial Least Squares Structural Equation Modelling (PLS-SEM), justifies the use of a smaller sample size. PLS-SEM yields results even with a small sample size (30 to 50 respondents), (Petter, 2018a).

4.1.9. Data analysis

Data analysis is central to any plausible study as it allows the researcher to organise and bring meaning to a large amount of data (Creswell, 2008). PLS-SEM is commonly used for quantitative data analysis and in explanatory studies where there is a need to get an understanding of a specific phenomenon (Bambale, 2014; Lowry & Gaskin, 2014) and due to the low sample size required in studies using this method of analysis (Petter, 2018b).

The distinction between PLS-SEM and the alternative method of SEM, CB-SEM, is minimal. These two approaches yield comparable results and need similar sample sizes, typically recommended to have a minimum of 200 participants (Dash & Paul, 2021a; Mohamad et al., 2008). The adoption of either method of analysis is a matter of preference (Dash & Paul, 2021b).

Data collected was exported from Qualtrics into the .cvs file format that was subsequently imported into the SmartPLS software package. SmartPLS was used for the quantitative analysis and to subsequently test the hypotheses of the study; using SmartPLS, the reliability, validity and structural model was evaluated.

4.1.9.1. Reliability

Reliability is used to assess measurement within a construct and is done by assessing composite reliability using PLS-SEM. Composite reliability is used to assess the internal consistency in scale items (Hair et al., 2014a). Another method which may be used is Cronbach's α however, this method may be less suitable using PLS-SEM (Hair et al., 2014b). Internal consistency is often used in positivist studies in Information Systems and assumes that the values in all items have the same range and understanding (Straub, 1989). By using SmartPLS, both the Cronbach's and Composite reliability were measured as is common in quantitative studies using structural equation modelling.

4.1.9.2. Validity

Construct validity is used to determine whether the method of measurement was suitable for the theory being measured (Bruce et al., 2008). Validity is examined by observing the construct's convergent validity and discriminant validity (Hair et al., 2014b). Methods often used in Information Systems studies to assess construct validity include discriminant validity, convergent validity and

factorial validity; the most common of these is factorial validity which assesses the convergent and discriminant validity (Straub, 1989). The factorial validity of the study was examined using SmartPLS and was achieved by assessing discriminant validity and convergent validity. The convergent validity was obtained by assessing the average variance extracted (AVE) whilst the discriminant validity was examined by using the Fornell-Larcker criterion measure as one of the methods (Straub, 1989; Urbach & Ahlemann, 2010).

4.1.9.3. Hypothesis test

T-tests are essential in testing hypotheses (Fay & Proschan, 2010). SmartPLS was used to conduct the t-test in order to test the hypotheses; bootstrapping was used to obtain the results of the hypotheses test (Kwong & Wong, 2013).

4.1.9.4. Operationalisation variables

The study used a cross-sectional survey for the collection of data. For the collected data to be precise, operationalisation of the variables was initiated for the measurement and analysis.

4.1.9.4.1. Dependent variables

A dependent variable is a data item whose value is influenced by the independent variable (Flannelly et al., 2014). The analysis had three dependent variables, namely, Policy Review, Policy Awareness and Compliance. It is postulated that Technostress, Information Overload and Job Insecurity negatively impact employees' Compliance, while Telecommuting will positively impact (organisational) Policy Review and Policy Awareness.

4.1.9.4.2. Independent variables

An independent variable is one that can be deliberately manipulated or the variable whose values are deliberately selected to observe the effects of the manipulation (Padilla, 1984). The analysis has four independent variables; these are Telecommuting, Technostress, Information Overload and Job Insecurity. The study postulates that the three independent variables, Job Insecurity, Technostress and Information Overload, have a negative impact on the compliance behaviour of employees, while Telecommuting has a positive impact on organisational Policy Awareness and organisational Policy Reviews.

4.1.9.4.3. Moderating variables

A moderating variable is one that affects the strength or weakness of the relation between the independent and dependent variables (Dewi & Monalisa, 2016). The analysis has two moderating variables, Fear and Telecommuting Intensity. This study postulates that Telecommuting Intensity will have a negative impact on the Compliance of employees when there is Information Overload and Technostress; additionally, altruistic fear associated with the pandemic will have a negative impact on the Compliance behaviour of employees when the job insecurity exists.

4.1.9.4.4. Control variables

Control variables in this study are Age, Gender, the Seniority Level of employees in organisations, Industry and Educational level. The control variables are shown to have a level of influence on the general compliance of employees, and therefore, there are benefits when these variables were controlled (Bansal & Shin, 2016; Solomon & Brown, 2021; Ullah Khan & Alshare, 2019).

4.1.9.4.5. Summary

Gaining a comprehensive understanding of the variables employed in a study is critical, followed by the identification of the scale utilised to measure the items pertaining to each construct., and the number of items to be measured for each variable; Table 8 shows the characteristics of each variable in this study.

Table 8. A summarisation of the variables for the study

Variable	Item	Measure	Scale
Telecommuting norm	TC	Four items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Telecommuting Intensity	TC1	Four items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Policy Review	PR	Four items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Policy Awareness	PA	Five items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Technostress	TS	Twelve items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Information Overload	IO	Four items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Altruistic fear	FR	Four items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Job insecurity	JI	Three items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Compliance	COMP	Four items	7-point Likert scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other.
Control variables	Numerous	Numerous	Nominal scales

4.1.9.5. Survey items

The construct items used in the questionnaire (see Table 9) were primarily drawn from previous studies. This study had 44 survey items, averaging five items per construct. The survey items are briefly discussed below.

4.1.9.5.1. Telecommuting norm

A recent study measured the impact of telecommuting in organisations using a seven-point Likert scale included a construct named "organisational norms on remote working" (Tanpipat et al., 2021). Although not exactly the same, this construct is similar in definition to the Telecommuting construct used in the study reported on here as both are related to the adoption of telecommuting in an organisation. This earlier study had seven items, however, only four items were adopted. The adopted items all start with "My organization …", but items that started with "My leader …" were excluded as this study wants to understand the impact of telecommuting in the organisational context.

Items of the construct related to telecommuting all passed the factor loadings, validity and reliability assessment, making them a good proposition for a study measuring work from home in organisations. This study presents questions such as "My organization has encouraged employees to work remotely when necessary".

4.1.9.5.2. Telecommuting intensity

Since no measurement items for high telecommuting intensity using the Likert scale were found, this study predominantly used items used found in a study on Facebook usage intensity (Ellison et al., 2007) This construct was used in studies on the impact of the intense use of Facebook on social capital (Ellison et al., 2007; vanden Abeele et al., 2018). Six items from this construct, which refer to the intensity or frequency of utilisation, were adopted. Excluded items are: "About how many total

Facebook friends do you have?" and "In the past week, on average, approximately how many minutes per day have you spent on Facebook?". The main reason for their exclusion is their use of the nominal scale. Another reason for their exclusion is that understanding the attitude of employees with regards to the extent of telecommuting will provide an understanding on how often employees work from home.
Two other excluded items were not applicable in a Likert scale as they are closed-ended and open-ended questions. Instead, the measurement items were modified and asked participants to agree or disagree with questions such as "Working from home is part of my everyday working arrangement".

4.1.9.5.3. Policy review

Policy maintenance in organisations was measured using a five-point Likert scale in the research reported on by Knapp & Ferrante (2012b). Policy maintenance is closely associated with policy review (Knapp et al., 2009) and this study opted to use the Policy Review construct to refer to maintenance of security policies in organisations. This was shown in the information security governance model (see Figure 1 in Section 2.2) to refer to the governance of information security in organisations (Knapp et al., 2009). Construct items were tested for convergent and discriminant validity and these items were found to be suitable. These items were measured using a seven-point Likert scale rather than a five-point scale to have a consistent measurement scale throughout the study. Construct items include questions like "In my organisation an information security policy that is consistently updated periodically would be beneficial".

4.1.9.5.4. Policy awareness

Similar to policy review in the section above, construct items for the Policy Awareness construct were derived from a previous study and present questions such as "In my organisation well-communicated information security awareness would be beneficial" (Knapp & Ferrante, 2012b).

4.1.9.5.5. Information overload

A proposed information overload scale which was assessed for reliability was used to measure the Information Overload construct and the items were modified to make them apply particularly to telecommuting in the context of work-from-home arrangements in organisations. Questions presented include, "I am often distracted by an excessive amount of information available to me as a result of telecommuting." (Zhang et al., 2016).

4.1.9.5.6. Technostress

The Technostress construct items were adopted and included questions such as "I am forced by this technology to do more work than I can handle" (Westermann, 2017). These items initially used a five-point Likert scale and had to be modified to the seven-point Likert scale adopted. This construct had 12 items that cover techno-overload, techno-invasion and techno-complexity. The ICT term in this study relates to digital technologies which include mobile technologies (e.g., mobile phones), network technologies (e.g., the internet) and communication technologies (e.g., e-mail).

4.1.9.5.7. Job insecurity

The Job Insecurity scale measures the construct items and initially used in a five-point Likert scale (vander Elst et al., 2014). However, in this study items from the validated Job Insecurity scale used a seven-point Likert scale and asked questions such as "Chances are, I will soon lose my job". The one reverse coded item was excluded as this study is using direct items and it would not benefit from using a reverse item (Suárez Álvarez et al., 2018).

4.1.9.5.8. Altruistic fear

Although a novel virus, several notable scales used to measure Altruistic Fear associated with COVID-19 do exist. One such scale (from Sloan et al. (2021)) was used and validated; questions

such as “I often worry about COVID-19 making people across South Africa sick” were presented. Although initially used on a four-point scale, a seven-point scale was adopted to maintain consistency.

4.1.9.5.9. Compliance

Construct items from a study on the information security policy compliance behavioural intentions of employees in organisations (from Ifinedo, (2014)) were used with a seven-point Likert scale. Construct items included “It is my intention to continue to comply with the organisation's information security policy”.

4.1.9.5.10. Control variables

This study has five control variables, namely Age, Gender, Industry, Educational Level and Seniority Level. The Seniority Level of employees variable was adopted from previous work (Roos & Van , 2008), and to fit with the context of South Africa the following seniority levels were defined and adopted:

- Senior management: These include CEOs, Managing Directors, Executive Directors and Heads of Departments.
- Middle management: Includes Line Managers and staff functioning in a relatively senior position on an individual basis in their specific functional units.
- Staff: All the other staff in an organisation.

All the other control variables are self-explanatory and easy to interpret as displayed in the table below.

Table 9. Measurement items for the study

Construct	Items	Source
Telecommuting norm (TC)	My organization has encouraged employees to work remotely when necessary	
	My organization has conducted technical training on remote work support.	
	My organization has focused on alternative flexible work arrangements and emerging support technologies.	
	My organization has involved remote work arrangement in the organization.	Tanpipat et al., 2021
Telecommuting Intensity (TCI)	Working from home is part of my everyday working arrangement.	
	Working from home has become part of my daily working arrangement.	
	I am proud to tell people that I frequently work from home.	Ellison et al., 2007
	I feel that I am part of the frequent work-from-home community.	
	I would be sorry if I stopped working from home.	
	I feel that I now mostly work from home.	
Policy Review (PR)	In my organisation an information security policy that is consistently updated on a periodic basis would be beneficial.	Knapp & Ferrante, 2012b
	In my organisation an information security policy should be updated when technology changes require it.	
	In my organisation an established information security policy review and update process would be essential.	
	In my organisation the security policy should be properly updated on a regular basis.	

Construct	Items	Source
Policy Awareness (PA)	My organisation would benefit if employees clearly understood the ramifications of violating security policies.	Knapp & Ferrante, 2012b
	In my organisation it would be helpful if necessary efforts are made to educate employees about new security policies.	
	In my organisation well communicated information security awareness would be beneficial.	
	In my organisation an effective security awareness would be important.	
	In my organisation, a continuous, ongoing security awareness program would absolutely be good.	
Technostress (TS)	I am forced by ICTs to do more work than I can handle.	Westermann, 2017
	I am forced by ICTs to work with very tight time schedules.	
	I am forced to change my habits to adapt to new ICTs.	
	I have a higher workload because of increased complexity of ICTs.	
	I have to be always available due to this technology.	
	I have to sacrifice time to keep current on new ICTs.	
	I feel my personal life is being invaded by ICTs.	
	I do not know enough about ICTs to handle it satisfactorily.	
	I need a long time to understand and use new ICTs.	
	I do not find enough time to study and upgrade my ICT skills.	
	I find others know more about this technology than I do.	
	I often find it too complex for me to understand and use new technology.	
Information Overload (IO)	I am often distracted by an excessive amount of information available to me as a result of telecommuting.	Zhang et al., 2016
	I find that I am overwhelmed by the amount of information I have to process on a daily basis as a result of telecommuting.	
	There is too much information due to telecommuting so I find it a burden to process.	
	I find that only a small part of the information while telecommuting is relevant to my needs.	
Altruistic Fear (FR)	I often worry about COVID-19 making my family members sick.	Sloan et al., 2021
	I often worry about COVID-19 making my friends sick.	
	I often worry about COVID-19 making the elderly I know sick.	
	I often worry about COVID-19 making my neighbours sick.	
	I often worry about COVID-19 making doctors and nurses sick.	
	I often worry about COVID-19 making people across South Africa sick.	
	I often worry about COVID-19 making people in other countries sick.	
Job Insecurity (JI)	Chances are, I will soon lose my job.	Van der Elst et al., 2014
	I feel insecure about the future of my job.	
	I think I might lose my job in the near future.	
	I would follow the organization's security policy whenever possible.	

Construct	Items	Source
Compliance (COM)	It is my intention to continue to comply with the organization's security policy.	Ifinedo, 2014
	I am certain I will adhere to my organization's security policy.	
	I am likely to follow the organization's security policy in the future.	
	I would follow the organization's security policy whenever possible.	
Gender	Male	Solomon & Brown, 2021
	Female	
	Prefer not to say	
Age	18-24	Solomon & Brown, 2021
	25-34	
	35-44	
	45-54	
	55 and above	
Industry	Academic/Education	Solomon & Brown, 2021
	Information Technology/Telecommunications	
	Manufacturing	
	Financial services	
	Engineering	
	Government	
	Retail	
	Healthcare	
	Other	
Educational level	Less than Matric	Hilmer & Futcher, 2019
	National Certificate (Matric) or equivalent	
	Higher certificate	
	Diploma & Advanced Certificate	
	Bachelor's Degree & Advanced Diploma	
	Honours Degree & Postgraduate Diploma	
	Master's degree	
	Doctoral degree	
Seniority level	Senior management	Roos & Van, 2008
	Middle management	
	Staff	

4.2. Ethical considerations

The researcher is fully aware of concerns pertaining to ethics in research; the researcher is also aware that anonymity is of paramount importance in studies of this nature. For this reason, the researcher specifies the following:

i. The researcher sought ethical approval from the University of Cape Town's Faculty of Commerce Ethics Board, the study commenced when it was approved.
ii. Anonymity is one of the significant concerns for participants in this study as well as organisations which the participants represent. Thus, the researcher did not include the names of participants or the organisations which employ participants.
iii. No participant were coerced into participating in the study, participation was entirely voluntary. Informed consent was conveyed to participants.

iv. All collected data was handled with the utmost confidentiality. All collected data was stored in a password protected storage area.

Appendices B and C have the ethics approval and clearance forms.

4.3. Pilot study

Pilot studies identify faults in the design and methods used in a study. Primary benefits of are that they help the researchers to check the survey instrument before the full-scale study commences, to understand how the data will be analysed and to fully understand the resources (time, human, costs etc.) that will be needed in the larger study (In, 2017; Malmqvist et al., 2019; Morin, 2013).

The pilot study had between 10-30 participants as recommended in previous studies (Hill & Hamilton, 1998; Isaac & Michael, 1995) to identify the most suitable items for the full-scale study. The pilot study commenced after ethics approval.

4.4. Possible limitations

The study is close ended; this may possibly be a limitation as an open-ended study may provide a richer understanding of compliance behaviour in organisations during the pandemic. The study was time-consuming, as it required at least 200 respondents to complete the questionnaire so as to provide sufficient data. This sample size is recommended for studies analysing the collected data using PLS-SEM.

Given the statistical nature of quantitative research, it is essential for the researcher, even with a non-statistics background, to be proficient in the use of statistics software and the underlying statistical methods. The researcher's training in statistics and data analysis was adequate for this study. Furthermore, the researcher possessed a level of familiarity with certain statistics software, which was advantageous.

4.5. Conclusion

This study adopted objectivism and positivism in its research design. Since the study presented hypotheses, the inductive research approach was adopted. The study was designed to look at measurable data and presented a conceptual model with constructs derived from previous studies. The study, being explanatory, approached the research with the aim of explaining causal relationships of variables. Findings are potentially significant in theory and practice and are expected to help in future understanding of the impact of the pandemic-induced contextual factors on the compliance behaviour of employees.

The study employed survey questionnaires as its research instrument. The data was collected using a 7-point Likert scale; the analyses was conducted using PLS-SEM due to the researcher’s familiarity with this method of analysis, its effectiveness and because this method is commonly used in Information Systems studies. The data was collected with the aid of Qualtrics Research Services. The respondents were employees in South African organisations that have adopted telecommuting and have information security policies in place. Purposive sampling was used.

The study used a cross-sectional survey for the collection of data. This study had three dependent variables, four independent variables and two moderating variables; this study also used control

variables in its operationalisation. Construct items were derived mainly from previous studies and were adapted specifically for this study. This study followed strict ethical considerations with anonymity and confidentiality guaranteed and all permission requirements duly followed. In the next chapter, the data collection process is described, and the results of the data analysis are presented.

5. Data analysis

This study utilised the PLS-SEM method of analysis using SmartPLS v. 3.3.3. PLS-SEM is commonly used in quantitative studies in Information Systems research due to its low sample size requirements and its innate capabilities to handle formative indicators (Petter, 2018b).

A total of 298 responses from employees in South African organisations which have information security policies were collected and analysed. The data was collected between 15 and 16 January 2022 using the methods and approaches described in Section 4. Responses were collected during the Omicron-fuelled COVID-19 surge in South Africa and the rest of the world and during the fourth wave of COVID-19 infections in South Africa when organisations required employees to work from home (Madhi et al., 2022).

This section presents the results of the analysis of the data which has been collected; there will be a subsection on the pre-analysis which discusses the measures taken before the actual analysis was conducted. Next, descriptive statistics, the measurement model, the structural model, the results of hypothesis testing, and a discussion of the findings are presented.

5.1. Pre-analysis

5.1.1. Data examination and preparation

Data examination and preparation are necessary to identify errors and duplications prior to analysis and allow the researcher to clean the collected data before commencing with data analysis (Powner, 2017).

The data was examined and prepared using the services offered by Qualtrics Research Services. However, further examination of the data was conducted by the researcher using Microsoft Excel. This examination did not yield any additional problems with the data, thus, the next step in the pre-analysis was initiated.

5.1.2. Pre-analysis of the measurement model

A pre-analysis of the data was conducted to help the researcher identify items that could not be used for the study and hence to help the researcher to do an accurate analysis that would represent reliable indicator values.

Outer loadings represent the single-headed arrows (see Figure 2) pointing from the latent construct to the indicator variables and are known as reflective indicators; these can be removed without changing the whole meaning of a construct (Hair et al., 2011, 2014a). However, outer loadings must be above the 0.7 maximum threshold value (Hair et al., 2017). The initial assessment of the measurement model showed that eight items' outer loadings (TS1, TS4, TS7, TS8, TS9, TS10, TS11, TS12) were very low (see Table 10), and as a result they had a negative impact on the reliability of the technostress construct (see Table 11 for the initial reliability and validity examination). These

items were thus deleted as recommended (Hair et al., 2014a). The model was then re-assessed, and all remaining constructs and measurement items passed the outer loadings assessment.

Table 10. Initial outer loadings

	COM	FR	IO	JI	ME1	ME2	ME3	PA	PR	TC	TCI	TS
AF1		0.882										
AF2		0.914										
AF3		0.886										
AF4		0.896										
AF5		0.916										
AF6		0.925										
AF7		0.878										
COMP1	0.941											
COMP2	0.927											
COMP3	0.930											
COMP4	0.903											
IO * TCI							1.033					
IO1			0.842									
IO2			0.928									
IO3			0.888									
IO4			0.859									
JI * FR					0.947							
JI1				0.899								
JI2				0.893								
JI3				0.952								
PA1								0.863				
PA2								0.900				
PA3								0.941				
PA4								0.928				
PA5								0.908				
PR1									0.854			
PR2									0.853			
PR3									0.899			
PR4									0.887			
TELE1										0.874		
TELE2										0.836		
TELE3										0.899		
TELE4										0.897		
TI1											0.961	
TI2											0.958	

	COM	FR	IO	JI	ME1	ME2	ME3	PA	PR	TC	TCI	TS
TI3											0.959	
TI4											0.961	
TI5											0.910	
TI6											0.939	
TS * TCI						0.982						
TS2												0.781
TS3												0.793
TS5												0.745
TS1												0.619
TS10												0.129
TS11												-0.002
TS12												-0.085
TS4												0.680
TS6												0.717
TS7												0.443
TS8												0.019
TS9												-0.019

Table 11. Initial reliability and validity of the construct

	Cronbach's Alpha	**rho_A**	**Composite Reliability**	**Average Variance Extracted (AVE)**
COM	0.944	0.945	0.960	0.856
FR	0.961	0.966	0.967	0.810
IO	0.908	1.011	0.932	0.774
JI	0.903	0.928	0.939	0.837
ME1	1.000	1.000	1.000	1.000
ME2	1.000	1.000	1.000	1.000
ME3	1.000	1.000	1.000	1.000
PA	0.947	0.948	0.959	0.825
PR	0.897	0.901	0.928	0.763
TC	0.900	0.908	0.930	0.769
TCI	0.978	0.986	0.982	0.899
TS	0.911	0.671	0.729	0.281

5.1.3. Survey items

After the pre-analysis, the approved survey items (see Table 12) were resubmitted to Qualtrics to be used for the collection of data. The approved survey items and the associated variables and their IDs are presented in Table 12.

Table 12. Final survey items

Construct	Construct ID	Items	Source
Telecommuting Norm (TC)	TN1	My organization has encouraged employees to work remotely when necessary	
	TN2	My organization has conducted technical training on remote work support.	
	TN3	My organization has focused on alternative flexible work arrangements and emerging support technologies.	
	TN4	My organization has involved remote working arrangement in the organization.	(Tanpipat et al., 2021)
Telecommuting Intensity (TCI)	TI1	Working from home is part of my everyday working arrangement.	
	TI2	Working from home has become part of my daily working arrangement.	
	TI3	I am proud to tell people that I frequently work from home.	(Ellison et al., 2007)
	TI4	I feel that I am part of the frequent work-from-home community.	
	TI5	I would be sorry if I stopped working from home.	
	TI6	I feel that I now mostly work from home.	
Policy Review (PR)	PR1	In my organisation an information security policy that is consistently updated on a periodic basis would be beneficial.	(Knapp & Ferrante, 2012b)
	PR2	In my organisation an information security policy should be updated when technology changes require it.	
	PR3	In my organisation an established information security policy review and update process would be essential.	
	PR4	In my organisation the security policy should be properly updated on a regular basis.	
Policy Awareness (PA)	PA1	My organisation would benefit if employees clearly understood the ramifications of violating security policies.	(Knapp & Ferrante, 2012b)
	PA2	In my organisation it would be helpful if necessary, efforts are made to educate employees about new security policies.	
	PA3	In my organisation well communicated information security awareness would be beneficial.	
	PA4	In my organisation an effective security awareness would be important.	
	PA5	In my organisation, a continuous, ongoing security awareness program would absolutely be good.	

Construct	Construct ID	Items	Source
Technostress (TS)	TS2	I am forced by ICTs to work with very tight time schedules.	(Westermann, 2017)
	TS3	I am forced to change my habits to adapt to new ICTs.	
	TS5	I have to be always available due to this technology.	
Information Overload (IO)	IO1	I am often distracted by an excessive amount of information available to me as a result of telecommuting.	(Zhang et al., 2016)
	IO2	I find that I am overwhelmed by the amount of information I have to process on a daily basis as a result of telecommuting.	
	IO3	There is too much information due to telecommuting so I find it a burden to process.	
	IO4	I find that only a small part of the information while telecommuting is relevant to my needs.	
Altruistic Fear (FR)	AF1	I often worry about COVID-19 making my family members sick.	(Sloan et al., 2021)
	AF2	I often worry about COVID-19 making my friends sick.	
	AF3	I often worry about COVID-19 making the elderly I know sick.	
	AF4	I often worry about COVID-19 making my neighbours sick.	
	AF5	I often worry about COVID-19 making doctors and nurses sick.	
	AF6	I often worry about COVID-19 making people across South Africa sick.	
	AF7	I often worry about COVID-19 making people in other countries sick.	
Job Insecurity (JI)	JI1	Chances are, I will soon lose my job.	(vander Elst et al., 2014)
	JI2	I feel insecure about the future of my job.	
	JI3	I think I might lose my job in the near future.	
Compliance (COM)	COMP1	It is my intention to continue to comply with the organization's security policy.	(Ifinedo, 2014)
	COMP2	I am certain I will adhere to my organization's security policy.	
	COMP3	I am likely to follow the organization's security policy in the future.	
	COMP3	I would follow the organization's security policy whenever possible.	
Gender		Male	(Solomon & Brown, 2021)
		Female	
		Prefer not to say	
Age		18-24	(Solomon & Brown, 2021)
		25-34	
		35-44	

Construct	Construct ID	Items	Source
		45-54	
		55 and above	
Industry		Academic/Education	(Solomon & Brown, 2021)
		Information Technology/Telecommunications	
		Manufacturing	
		Financial services	
		Engineering	
		Government	
		Retail	
		Healthcare	
		Other	
Educational Level		Less than Matric	(Hilmer & Futcher, 2019)
		National Certificate (Matric) or equivalent	
		Higher certificate	
		Diploma & Advanced Certificate	
		Bachelor's Degree & Advanced Diploma	
		Honours Degree & Postgraduate Diploma	
		Master's degree	
		Doctoral degree	
Seniority Level		Senior management	(Roos & Van, 2008)
		Middle management	
		Staff	

In the next section, the descriptive statistics will be presented; this includes the demographic distribution of the participants in this study.

5.2. Descriptive statistics

Descriptive statistics help the researcher to summarise data in an organised manner by providing a description of the relationship between the variable and the population. They provide descriptions of the characteristics of a given sample (Fisher & Marshall, 2009; Kaur et al., 2018). The indicators in this study did not have any missing values as the participants (N=298) completed all the questions presented to them. This section summarises the construct items of variables for the data collected and will help us understand the central tendency, or mean and median, of the indicator values relative to the seven-point Likert scale adopted (this is important in a descriptive analysis) (Fisher & Marshall, 2009).

5.2.1. Telecommuting norm

The average value of indicators for the Telecommuting norm construct is above point 4 on the seven-point Likert scale (see Table 13), which suggests that the adoption of work-from-home arrangements in organisations is high. This indicates that most of the organisations had telecommuting.

Table 13. Telecommuting norm descriptive statistics

	No.	Missing	Mean	Median	Min
TELE1	6	0	5.221	6	1
TELE2	7	0	4.829	5	1
TELE3	8	0	5.238	6	1
TELE4	9	0	5.265	6	1

5.2.2. Telecommuting intensity

Values of indicators for the Telecommuting Intensity variable are all above the mid-level point of the seven-point Likert scale (see Table 14). and show that there is telecommuting intensity in organisations. This may be explained by the period at the height of the pandemic when the data was collected.

Table 14. Telecommuting intensity descriptive statistics

	No.	Missing	Mean	Median	Min
TI1	10	0	4.262	5	1
TI2	11	0	4.319	5	1
TI3	12	0	4.218	5	1
TI4	13	0	4.201	5	1
TI5	14	0	4.074	5	1
TI6	15	0	4.000	4	1

5.2.3. Policy review

The values of indicators in the Policy Review are well above the average point in the seven-point Likert scale, which suggests that policy review procedures in organisations are significant, indicating that the review of information security policies is well received in organisations (see Table 15).

Table 15. Policy Review descriptive statistics

	No.	Missing	Mean	Median	Min
PR1	16	0	5.594	6	1
PR2	17	0	5.711	6	1
PR3	18	0	5.738	6	1
PR4	19	0	5.883	6	1

5.2.4. Policy awareness

Similar to the values of indicators in Policy Review, Policy Awareness values are significantly above the mid-level point in the seven-point Likert scale, suggesting the existence of policy awareness in organisations among employees. Importantly, these values also indicate that policy awareness is well received in the organisations (see Table 16).

Table 16. Policy Awareness descriptive statistics

	No.	Missing	Mean	Median	Min
PA1	20	0	5.933	6	1
PA2	21	0	6.064	6	1
PA3	22	0	6.101	6	1
PA4	23	0	6.057	6	1
PA5	24	0	6.020	6	1

5.2.5. Information overload

Most of the values of Information Overload indicators are just above the mid-level point of the seven-point Likert scale, which suggests that there is a moderate level of information overload among employees in organisations (see Table 17).

Table 17. Information Overload descriptive statistics

	No.	Missing	Mean	Median	Min
IO1	37	0	4.023	4	1
IO2	38	0	3.926	4	1
IO3	39	0	3.775	4	1
IO4	40	0	4.131	4	1

5.2.6. Technostress

All values of the indicators in the Technostress variable are above the mid-level point of the Likert scale suggesting the existence of technostress (see Table 18).

Table 18. Technostress descriptive statistics

	No.	Missing	Mean	Median	Min
TS2	26	0	3.923	4	1
TS3	27	0	4.463	5	1
TS5	29	0	4.732	5	1

5.2.7. Altruistic fear

All the values of the indicators in the Altruistic Fear variable are significantly above the mid-level point of the seven-point Likert scale, suggesting that altruistic fear is pronounced among participants in this study (see Table 19).

Table 19. Altrustic Fear descriptive statistics

	No.	Missing	Mean	Median	Min
AF1	41	0	5.671	6	1
AF2	42	0	5.570	6	1
AF3	43	0	5.866	6	1
AF4	44	0	5.299	6	1
AF5	45	0	5.591	6	1
AF6	46	0	5.456	6	1
AF7	47	0	5.279	6	1

5.2.8. Job insecurity

Only one Job Insecurity indicator has values that are above the mid-level point of the seven-point Likert scale, suggesting that job insecurity is not significantly experienced among many participants in this study, indicating that participants do not feel that their jobs are at risk (see Table 20).

Table 20. Job Insecurity descriptive statistics

	No.	Missing	Mean	Median	Min
J11	48	0	2.993	3	1
J12	49	0	3.782	4	1
J13	50	0	3.268	3	1

5.2.9. Compliance

All the values in the indicators of the Compliance variable are significantly above the mid-level point of the seven-point Likert scale, suggesting that compliance is *not* an issue amongst participants in this study. This suggests that the vast majority of participants believe that they are compliant with information security policies (see Table 21).

Table 21. Compliance descriptive statistics

	No.	Missing	Mean	Median	Min
COMP_1	51	0	6.171	6	1
COMP_2	52	0	6.097	6	1
COMP_3	53	0	6.134	6	1
COMP_4	54	0	6.154	6	1

5.2.10. Distribution of demographic statistics

Demographic statistics generally consist of gender, age and education level. An understanding of the demographic statistics will helps the researcher to understand the composition of the sample of participants. This section looks at the distribution of the general demographic statistics (N=298) to get an understanding of the ages, gender, levels of education, seniority in their organisations and the industry in which the participants are employed.

5.2.10.1. Gender

The number of female participants is significantly greater than the number of male participants, with 58.1% of the participants female and 41.9% male. Previous studies have shown the overrepresentation of females in studies of this nature (Ameen et al., 2020a; Anwar et al., 2017); these numbers are shown in Table 22.

Table 22. Gender statistics results

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	125	41.9	41.9	41.9
	Female	173	58.1	58.1	100.0
	Total	298	100.0	100.0	

5.2.10.2. Age

The largest group of participants were between the ages of 25-34 at 47%, with participants between the ages of 35-44 second at 31.5%. There were fewer participants between the ages of 45-54, 18-24 and 55 or above at 9.7%, 7% and 4.7% (see Table 23).

Table 23. Statistics of the age of participants

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18 - 24	21	7.0	7.0	7.0
	25 - 34	140	47.0	47.0	54.0
	35 - 44	94	31.5	31.5	85.6
	45 - 54	29	9.7	9.7	95.3
	55 and above	14	4.7	4.7	100.0
	Total	298	100.0	100.0	

5.2.10.3. Seniority level

Most participants (46%) were ordinary (not management level) staff in organisations, while 38.9% were middle management staff members and there were (15.1%) senior management staff (See Table 24). The proportions of staff in the organisations from which the participants come are unknown but is predictable that there are fewer staff members at each more senior level.

Table 24. Seniority level statistics

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Senior management	45	15.1	15.1	15.1
	Middle management	116	38.9	38.9	54.0
	Staff	137	46.0	46.0	100.0
	Total	298	100.0	100.0	

5.2.10.4. Education level

Bachelor's degree together with Advanced diploma and National certificates were the most common qualifications held by participants at 28.2% and 26.8%, respectively. Diploma or Advanced certificates and Higher certificates (17.4% and 12.4% respectively) were third and fourth most common. Relatively few participants held Honours, Masters and Doctoral degrees (9.4%, 5% and 0.7%, respectively). Table 25 shows the educational level statistics. This distribution is fairly typical across organisations in South Africa.

Table 25. Education level statistics

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	National Certificate (Matric) or equivalent	80	26.8	26.8	26.8
	Higher certificate	37	12.4	12.4	39.3
	Diploma & Advanced certificate	52	17.4	17.4	56.7
	Bachelor's degree & Advanced diploma	84	28.2	28.2	84.9
	Honours degree & Postgraduate diploma	28	9.4	9.4	94.3
	Master's degree	15	5.0	5.0	99.3
	Doctoral degree	2	0.7	0.7	100.0
	Total	298	100.0	100.0	

5.2.10.5. Industry

Most participants worked in unspecified industries (23.8%), financial services had the second most participants (17.1%), with Information Technology/Telecommunications coming third (15.8) (see Table 26).

Table 26. Industry statistics

		Frequency	%	Valid %	Cumulative %
Valid	Academic/Education	22	7.4	7.4	7.4
	Information Technology/ Telecommunications	47	15.8	15.8	23.2
	Manufacturing	22	7.4	7.4	30.5
	Financial services	51	17.1	17.1	47.7
	Engineering	17	5.7	5.7	53.4
	Government	20	6.7	6.7	60.1
	Retail	29	9.7	9.7	69.8
	Healthcare	19	6.4	6.4	76.2
	Other	71	23.8	23.8	100.0
	Total	298	100.0	100.0	

5.3. Measurement model

The measurement model is the method that is used in Structural Equation Modelling to examine the relationship between the latent variables and their measure items (Bartholomew, 1993). The validity and reliability of construct items is usually assessed (Schmidt et al., 2000). This paper also assesses the indirect effects and outer loadings.

5.3.1. Assessment of convergent validity

Convergent validity is used to measure how closely related a scale is to variables and measures of the same construct. In PLS-SEM, a common method used in measuring convergent validity is Average Variance Extracted (AVE) (Carlson & Herdman, 2012; Cheah et al., 2018; Mohamad et al., 2008). Acceptable convergent validity is normally considered to be between 0.7 and 0.8, and most items were found to be in that range when rounded although two (COM - compliance and PA – policy awareness) are above 0.85 (however, not above 0.9), which suggests that variables have excellent convergent validity (Cheung & Wang, 2017). Table 27 shows the results of the assessment.

Table 27. The assessment of the convergent validity using AVE

	Average Variance Extracted (AVE)	Remark
COM	0.856	Acceptable
FR	0.810	Acceptable
IO	0.774	Acceptable
JI	0.837	Acceptable
ME1	0.825	Acceptable
ME2	0.763	Acceptable
ME3	0.736	Acceptable
PA	0.899	Acceptable
PR	0.769	Acceptable

5.3.2. Measurement of internal consistency

Internal consistency is a measure of scale reliability. Essentially, it measures whether items that measure the same general construct yield similar scores (Hair et al., 2011). Common methods used in measuring internal consistency are Cronbach's alpha, rho_A and composite reliability (Ferketich, 1990; Vehkalahti et al., 2006). Most items had composite reliability, rho_A and Cronbach's Alpha between 0.7 and 0.9, which is considered excellent or acceptable internal consistency, with a few between 0.91 and 0.98, which is considered high (Aguirre-Urreta et al., 2013; Aimran et al., 2008). These figures can be seen in Table 28.

Table 28. Measurement of the internal consistency

	Cronbach's Alpha	**rho_A**	**Composite Reliability**	**Remark**
COM	0.944	0.945	0.960	High but acceptable
FR	0.961	0.966	0.967	High but acceptable
IO	0.908	1.011	0.932	High but acceptable
JI	0.903	0.928	0.939	High but acceptable
ME1	0.947	0.948	0.959	High but acceptable
ME2	0.897	0.901	0.928	Acceptable
ME3	0.825	0.848	0.893	Acceptable
PA	0.978	0.985	0.982	High but acceptable
PR	0.900	0.908	0.930	High but acceptable

5.3.3. Discriminant validity

Discriminant validity refers to the extent the measures of different constructs are distinct (Mikhalkin et al., 2017). The methods used in the assessment of the discriminant validity were the Fornell-Larcker criterion and the Heterotrait-Monotrait Ratio (HTMT). The Fornell–Larcker criterion dictates that the square root of the AVE of every construct must be greater than the construct's highest correlation with any other construct in the model; the HTMT, on the other hand, is an estimate of the factor correlation (Mikhalkin et al., 2017). For discriminant validity to exist, in an HTMT measure (see Table 30), values must be below 0.9 (Franke & Sarstedt, 2019; Mikhalkin et al., 2017). All constructs in the study have a value below 0.9, suggesting the existence of discriminant validity. Table 29 shows the results of the Fornell-Larcker criterion assessment.

Table 29. Fornell-Larcker Criterion measure result

	COM	FR	IO	JI	ME1	ME2	ME3	PA	PR	TC	TCI	TS
COM	0.925											
FR	0.280	0.900										
IO	0.019	0.130	0.880									
JI	-0.062	0.147	0.342	0.915								
ME1	0.040	-0.165	0.041	0.216	1.000							
ME2	-0.009	-0.083	0.092	-0.012	0.143	1.000						
ME3	-0.091	-0.058	0.136	0.182	0.142	0.436	1.000					
PA	0.567	0.212	-0.013	-0.021	0.065	0.006	-0.075	0.908				
PR	0.526	0.144	-0.008	-0.061	0.075	0.026	-0.043	0.735	0.874			
TC	0.320	0.184	-0.123	-0.075	0.085	-0.024	0.046	0.354	0.543	0.877		
TCI	0.153	0.067	-0.068	-0.016	-0.051	0.004	0.039	0.176	0.327	0.575	0.948	
TS	0.185	0.172	0.388	0.175	-0.013	-0.013	0.092	0.160	0.133	0.083	0.187	0.858

Table 30. Heterotrait-Monotrait Ratio measure result

	COM	FR	IO	JI	ME1	ME2	ME3	PA	PR	TC	TCI	TS
COM												
FR	0.290											
IO	0.027	0.132										
JI	0.067	0.154	0.380									
ME1	0.040	0.168	0.047	0.229								
ME2	0.035	0.085	0.103	0.014	0.143							
ME3	0.093	0.057	0.143	0.191	0.142	0.436						
PA	0.599	0.222	0.032	0.029	0.067	0.021	0.077					
PR	0.570	0.153	0.048	0.069	0.080	0.032	0.046	0.800				
TC	0.343	0.195	0.142	0.107	0.092	0.029	0.048	0.379	0.595			
TCI	0.157	0.066	0.060	0.039	0.052	0.014	0.041	0.182	0.347	0.611		
TS	0.209	0.185	0.462	0.206	0.017	0.041	0.109	0.176	0.149	0.097	0.196	

5.3.4. Indirect effects

Indirect effects are used in PLS-SEM to test the presence of a mediating construct (Memon et al., 2018). A mediating variable helps explain the process in which two variables are related (MacKinnon, 2015). In the table below (Table 31) indirect effects were assessed for their statistical significance in order to identify any possible mediating variable. It was found that Telecommuting Norm, Policy Reviews and Policy Awareness are related relative to Compliance. This indicates that information security governance can be a mediating construct in understanding the impact of telecommuting on information security policies compliance. The results of the indirect effect test can be seen in Table 31.

Table 31. Results of the assessment of the indirect effects

	Original Sample	Sample Mean	Standard Deviation	t-Value	p-Value
TC -> PA -> COM	0.119	0.125	0.045	2.628	0.009
FR -> JI -> COM	-0.012	-0.013	0.011	1.131	0.258
TC -> PR -> COM	0.126	0.121	0.050	2.526	0.012
TCI -> IO -> COM	0.000	0.000	0.006	0.031	0.975
TCI -> TS -> COM	0.017	0.018	0.011	1.563	0.118

5.3.5. Outer loadings

As defined in Section 5.1.2, outer loadings represent the single-headed arrows (Figure 2) pointing from the latent construct to the indicator variables and are known as reflective indicators and these can be removed without impacting a construct. After the pre-analysis assessment of the model in Section 5.1.2, a further assessment was conducted to estimate the relationship in the reflective measurement model. This was conducted before the analysis for internal consistency and convergent validity after the deletion of measurement items which scored low in the initial assessment. The minimum threshold value for outer loadings is 0.70 (Hair et al., 2011, 2014a) and all construct items scored higher than 0.70, Hence the outer loadings in this study are acceptable. The outer loadings assessment results can be seen in Appendix D.

5.4. Structural model assessment

The structural model is assessed after the measurement of the model (Nanayakkara & Peiris, 2017) (see Figure 4 for the structural model). Several methods are used to assess the structural model in PLS-SEM studies, namely, R-square values, Normed Fit Index (NFI) and Standardized Root Mean Square Residual (SRMR) (Hair et al., 2017). Other methods such as the degree of freedom (df), Goodness Fit Index (GFI) and the Adjusted Good of Fit Index (AGFI) are normally applied in studies utilising CB-SEM (Dash & Paul, 2021b; Hair et al., 2017). The measurement in Section 4.3 gave solid support of the model presented in this study.

As noted above, when conducting an analysis of a model in the social sciences using PLS-SEM, common methods used in the assessment of the goodness of fit are R2, NFI, SRMR (Dash & Paul, 2021b). For the measurement of the R2 values, R2 values of 0.12 or below indicate low, between 0.13 to 0.25 values indicate medium, 0.26 or above indicate a high effect size (Cohen, 1992). As can be seen in Table 32 the Compliance and Policy Awareness variables have high effect sizes whilst the Policy Review is just slightly above the low range (see Table 32). Other studies have suggestions for acceptable r-squared values; using these it is seen that the values of the variables in this study generally have R2 values varying from strong to low suggesting that the strength of the relationship between the linear model and the three dependent variables is acceptable.

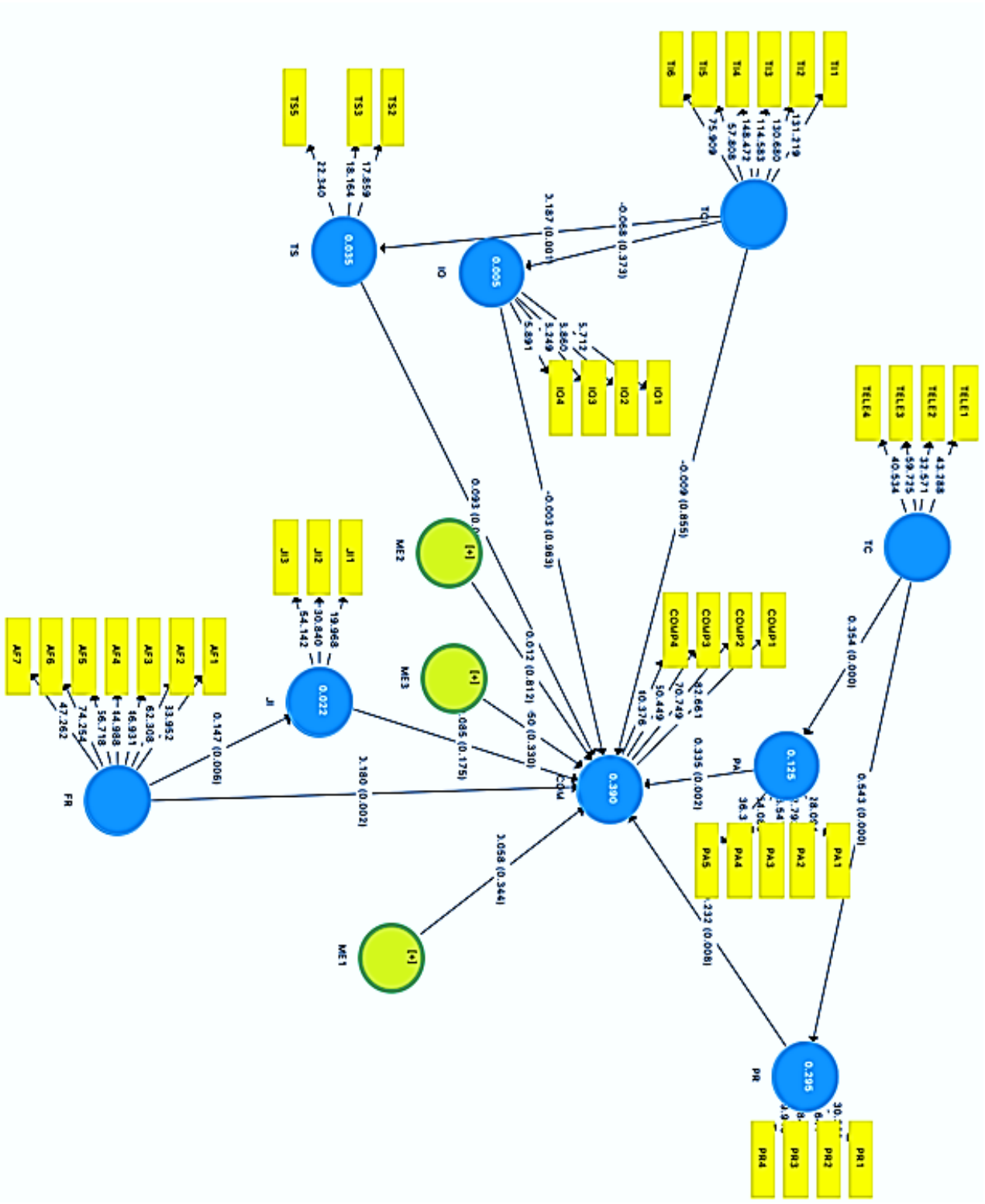

Figure 4. Structural model of the study imported from SmartPLS.

Table 32. The values of the R2 measure

	R Square	R Square Adjusted	Remark
COMP	0.391	0.369	Acceptable
PA	0.125	0.122	Low but Acceptable
PR	0.295	0.293	Acceptable

SmartPLS displays both saturated and estimated models, but a limited number of studies appear to have been conducted to understand the difference between these and the definitions of these two outcomes are vague (Hair et al., 2019). Although the most reasonable choice seems to be the estimated model, it may be assumed that it is at the discretion of the researcher to display the value that he or she believes is the most suitable (Hair et al., 2019). In this study, the model had a SRMR value of 0.042 for the saturated model; it is suggested that the lower the SRMR, the better, preferably, lower than 0.1, which suggests that the SRMR is acceptable. An acceptable NFI would be close to 1, with 0.9 considered to be acceptable (Dash & Paul, 2021b). The NFI value for this model is 0.86, which is very close to 0.9 and borderline acceptable. These figures can be seen in Table 33.

Table 33. SRMR and NFI assessment results

	Saturated Model	Estimated Model	Remark
SRMR	0.039	0.109	Acceptable
NFI	0.851	0.816	Borderline acceptable

This study could not conduct other methods of assessing the structural model as AGFI, df and GFI as the methods adopted for the study are PLS-SEM and not CB-SEM. Some studies suggest that CB-SEM is better than PLS-SEM at assessing goodness of fit, however for a study with a moderate sample size, it may be more suitable to conduct analysis using PLS-SEM (Dash & Paul, 2021b; Hair et al., 2017). Essentially both methods of analysis are suitable in an Information Systems study. Methods that were used in the assessment of the structural model are efficient for Information Systems research and it can be concluded that the assessment of the structural model showed that the model is a good fit.

Variance inflation factor

The variance inflation factor (VIF) is a measure of the extent of multi-collinearity in a group of multiple regression variables; this measure indicates the increase in the variance of a regression coefficient due to collinearity (Götz et al., 2010; Stine, 1995). All VIF values in this study are between 0.2- and 5.00, as recommended (Kwong & Wang, 2013), and this indicates that the structural model has no collinearity among the predictor constructs. The results of this assessment can be seen in Table 34.

Table 34. VIF statistics result

	COM	FR	IO	JI	ME1	ME2	ME3	PA	PR	TC	TCI	TS
COM												
FR	1.152			1.000								
IO	1.357											
JI	1.275											
ME1	1.146											
ME2	1.283											
ME3	1.320											
PA	2.299											
PR	2.416											
TC								1.000	1.000			
TCI	1.201		1.000									1.000
TS	1.296											

5.5. Moderation analysis

A moderating variable impacts the relationship between a dependent variable and an independent variable (De Souzabido & Da Silva, 2019). In the analysis of the moderating variable, Telecommuting Intensity showed a positive slope in the relationship between Technostress and Compliance (ME2) (Moderation effect 2 in Figure 6), suggesting that the higher the Telecommuting Intensity, the higher the Technostress. As a consequence, Technostress negatively impacts Compliance behaviour. However, Altruistic Fear (ME1) (Moderation effect 1 in Figure 5) and Information Overload (ME3) (Moderation effect 3 in Figure 7) display negative slopes.
The next section will look at the impact of the moderating effects on the compliance behaviour of employees by looking at the statistical significance of the moderation variables as well as the general hypotheses test results of the study.

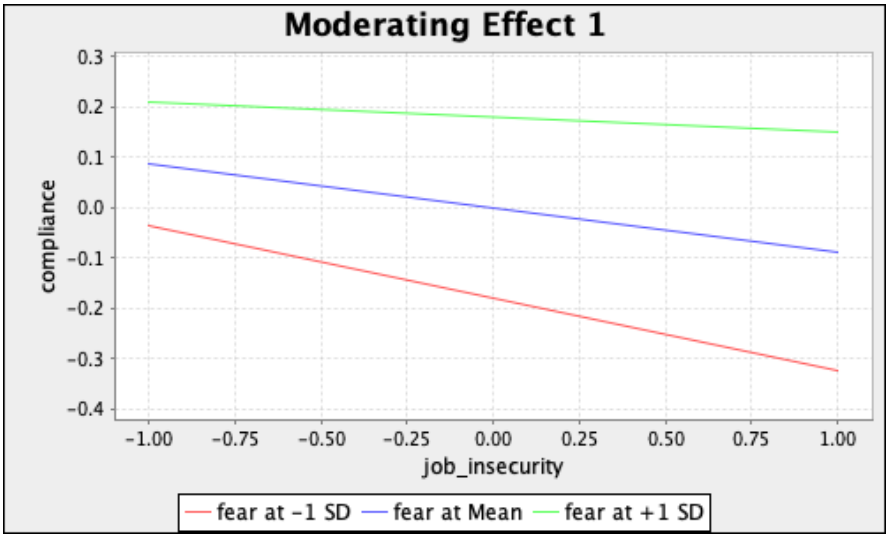

Figure 5. Moderation effect 1 slope.

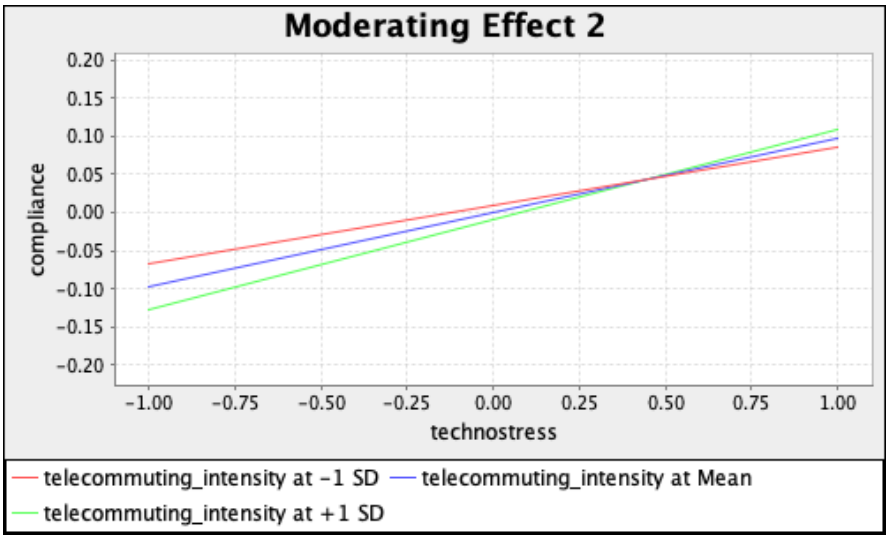

Figure 6. Moderation effect 2 slope.

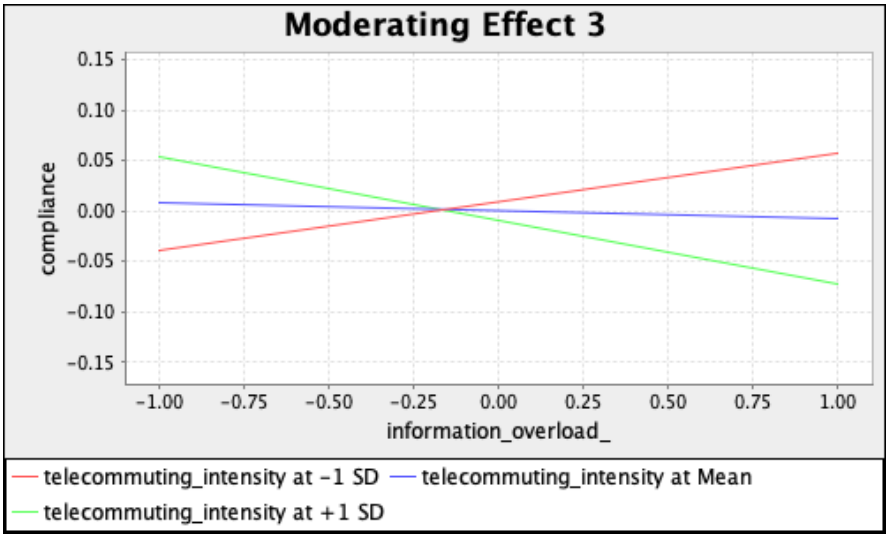

Figure 7. Moderation effect 3 slope.

5.6 Hypotheses test results

The findings answer the research questions and that aids in understanding the research problem. The test was conducted using the bootstrapping method with the recommended subsample of 5000 - the bootstrapping method is used to draw a significant number of subsamples from the original data. The statistical significance t-values and p-values are used to determine the significance of indicator weights and to subsequently test the hypotheses (Hair et al., 2014a; Kwong & Wong, 2013; Streukens & Leroi-Werelds, 2016). The path coefficients help to indicate the direct effect of a variable that has been assumed to be the cause on another variable that has been assumed to be an effect (Auriacombe, 2007). These help to establish the correlation of a variety of variables in a model.

The hypotheses tests were used a two-tailed test with the significance levels of 0.05, 0.01, 0.5, and 0.1. Although the statistical significance level of 0.1 is not as frequently used as the other levels, it can be applied in a study of the nature of this study to determine the statistical significance of the hypotheses as authors in the field of probability have noted that the level is an arbitrary decision (Cowles & Davis, 1982; Gelman & Stern, 2012). This justifies the use of the statistical levels mentioned in this study.

The results show that five of the hypotheses in this study were supported. Although the moderating effect was not statistically significant, in the following section, the statistical significance of the three moderating effects as well as the other hypotheses will be examined in greater depth by conducting a multigroup analysis to understand the hypotheses test results.

As displayed in Table 35 below, H3, H4, H5, H7 and H8 were not supported; however, H1, H2, H6 and H9a and H9b are supported at a statistical significance level of 0.05, with H6 also supported at a statistical significance level of 0.05, although its P value is 0.053 (it is approaching borderline significance) (Thiese et al., 2016). The hypotheses results are displayed in Table 35 and Figure 8 is a diagram of the hypotheses test results.

Table 35. Hypotheses test results

		Path coefficients	**t-Value**	**p-Value**	**Result**
H1	TC -> PA	0.354	5.474	0.000	Supported
H2	TC -> PR	0.543	10.772	0.000	Supported
H3	ME3 -> COM	-0.050	0.975	0.330	Not supported
H4	ME2 -> COM	0.012	0.238	0.812	Not supported
H5	IO -> COM	-0.003	0.046	0.963	Not supported
H6	TS -> COM	0.093	1.935	0.053	Supported
H7	JI -> COM	-0.085	1.356	0.175	Not supported
H8	ME1 -> COM	0.058	0.946	0.344	Not supported
H9a	PA -> COM	0.335	3.088	0.002	Supported
H9b	PR -> COM	0.232	2.653	0.008	Supported

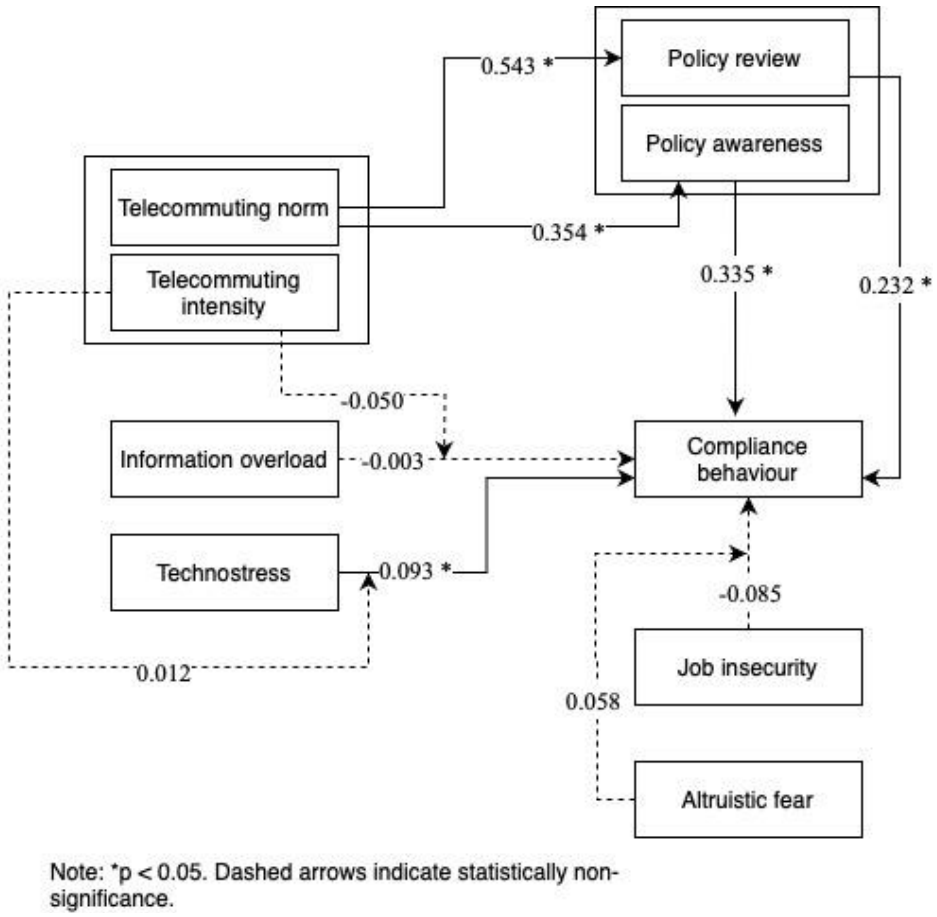

Figure 8. Model of the hypotheses test results.

Multigroup analysis

A separate multigroup analysis was conducted to get a deeper understanding of the hypotheses test by looking at the subgroups in the study population. The subsequent analysis does not answer the research questions, but it aims to provide an understanding of the phenomenon from a heterogeneous perspective as is important in the security area where we are studying populations with different experiences influenced by diverse factors.

A multigroup analysis was conducted to test the hypotheses according to the genders and age groups of the participants in order to identify potential differences in the hypotheses test results and get a more specific understanding of the hypotheses test results.

Multigroup analysis is especially useful in understanding results in populations that are heterogeneous (Henseler, 2007, 2012). Previous studies that have reported on the compliance behaviour of employees in organisations looked at the impacts of gender and age on the compliance behaviour amongst employees (Ameen et al., 2020b; Anwar et al., 2017; Guhr et al., 2018). A multigroup analysis will was expected to help us to understand this phenomenon by looking at the impact of selected subgroups on compliance.

The variables to be analysed in the multigroup analysis were available from the set of control variables and were adopted as the individual differences of the sub-populations to be analysed.

A three-step process was followed, and measurement invariance of composite models (MICOM) analysis was conducted following a rigorous process in the multigroup analysis. The MICOM procedure is utilised in safeguarding the validity of outcomes and conclusions in composite modelling in PLS-Path Modelling (Jun-Hwa et al., 2020; Matthews, 2017).

After establishing Step 1, which is to determine identical data treatment, Step 2 of the MICOM analysis (composite invariance) was conducted (see Table 36); this step is necessary to ensure that the prescription for condensing the indicator variables into composites is the same for all groups (Jun-Hwa et al., 2020). Results seen in this table show that only one failed to establish composite invariance.

Table 36. Step 2 of the MICOM

	Original Correlation	**Correlation Permutation Mean**	**10.0%**	**Permutation p-Values**
COM	1.000	1.000	1.000	0.487
FR	1.000	0.999	0.998	0.537
IO	0.994	0.885	0.615	0.860
JI	0.999	0.993	0.983	0.747
ME1	1.000	1.000	1.000	0.050
ME2	1.000	1.000	1.000	0.217
ME3	1.000	1.000	1.000	0.433
PA	1.000	1.000	0.999	0.683
PR	1.000	0.999	0.999	0.470
TC	1.000	0.999	0.998	0.743
TCI	1.000	1.000	0.999	0.307
TS	0.999	0.991	0.977	0.847

Finally, Step 3 (see Appendix E) was conducted to establish the equality of the composites' mean values and variances (Jun-Hwa et al., 2020). Most of the variables were able to establish the equality of the mean values and variances of the composites. The results of the multigroup analysis for the Gender subgroup (see Table 37) were mixed, however, the results show that gender has an effect on compliance behaviour.

The subsequent multigroup analysis, which will feature in this section, also followed the same rigorous process and the findings were checked, and all three steps of the MICOM analysis were satisfactory; thus, in this section, only the final results will be shown of the multigroup analysis for age groups of the participants of this study.

Table 37. Gender multigroup analysis results

	Path Coefficients Original (Female)	Path Coefficients Original (Male)	Path Coefficients Mean (Female)	Path Coefficients Mean (Male)	t-Value (Female)	t-Value (Male)	p-Value (Female)	p-Value (Male)
FR -> COM	0.149	0.214	0.154	0.204	1.758	2.472	0.079	0.013
FR -> JI	0.099	0.207	0.111	0.212	1.151	2.419	0.250	0.016
IO -> COM	0.044	-0.046	0.042	-0.062	0.650	0.500	0.515	0.617
JI -> COM	-0.143	0.001	-0.144	0.005	1.380	0.014	0.168	0.989
ME1 -> COM	0.030	0.094	0.033	0.083	0.238	1.325	0.812	0.185
ME2 -> COM	-0.061	0.116	-0.061	0.108	0.844	1.355	0.399	0.175
ME3 -> COM	-0.008	-0.164	-0.004	-0.146	0.145	1.712	0.884	0.087
PA -> COM	0.250	0.519	0.284	0.524	1.799	3.154	0.072	0.002
PR -> COM	0.256	0.146	0.234	0.158	2.864	0.867	0.004	0.386
TC -> PA	0.297	0.420	0.301	0.422	3.518	4.493	0.000	0.000
TC -> PR	0.509	0.583	0.512	0.587	6.843	8.802	0.000	0.000
TCI -> COM	-0.006	-0.001	-0.004	-0.005	0.091	0.014	0.927	0.989
TCI -> IO	-0.036	-0.090	-0.033	-0.093	0.318	0.799	0.750	0.424
TCI -> TS	0.163	0.233	0.170	0.245	2.013	2.603	0.044	0.009
TS -> COM	0.151	0.022	0.147	0.022	2.565	0.248	0.010	0.805

Table 38. Multigroup analysis results of the age subgroups

	Path Coefficients Original (age18_34(3.0))	Path Coefficients Original (age35(4.0))	Path Coefficients Mean (age18_34(3.0))	Path Coefficients Mean (age35(4.0))	t-Value (age18_34(3.0))	t-Value (age35(4.0))	p-Value (age18_34(3.0))	p-Value (age35(4.0))
FR -> COM	0.195	0.116	0.204	0.126	2.404	1.515	0.016	0.130
FR -> JI	0.071	0.250	0.077	0.254	0.745	3.158	0.456	0.002
IO -> COM	0.001	0.006	-0.009	-0.017	0.016	0.077	0.988	0.939
JI -> COM	-0.040	-0.195	-0.046	-0.172	0.441	2.259	0.660	0.024
ME1 -> COM	-0.051	0.181	-0.042	0.165	0.547	2.148	0.585	0.032
ME2 -> COM	0.098	-0.126	0.095	-0.110	1.357	1.913	0.175	0.056
ME3 -> COM	-0.128	0.127	-0.118	0.089	1.819	1.927	0.069	0.054
PA -> COM	0.250	0.488	0.269	0.503	1.640	3.446	0.101	0.001
PR -> COM	0.268	0.245	0.256	0.223	1.910	2.223	0.056	0.026
TC -> PA	0.441	0.254	0.439	0.260	5.218	3.231	0.000	0.001
TC -> PR	0.569	0.524	0.569	0.527	8.668	7.227	0.000	0.000
TCI -> COM	-0.048	-0.020	-0.043	-0.025	0.716	0.315	0.474	0.752
TCI -> IO	-0.094	0.002	-0.099	-0.021	0.985	0.017	0.325	0.987
TCI -> TS	0.069	0.334	0.070	0.341	0.748	4.592	0.454	0.000
TS -> COM	0.096	0.149	0.102	0.138	1.449	2.250	0.147	0.025

A second multigroup analysis was conducted using the Age subgroups; this study looked at two important age groups, participants between the ages of 18 and 34 (N=161) and participants aged 35 and above (N=137); these two age groups were selected to get an understanding of the compliance behaviours of Millennials and Gen Xs. Findings were very revealing as most of the hypotheses were supported for participants aged 35 and above, this suggests that COVID-19 pandemic-induced contextual factors have an impact on those that are considered to be Gen X and middle-aged, the results of the multigroup analysis can be seen in Table 38.

5.7. Research findings

The findings from this study show that COVID-19 pandemic-induced contextual factors have a significant impact on the compliance behaviour of individuals in organisations. The empirical findings are of value since few similar studies have been conducted.

The study found that telecommuting has a positive impact on aspects of information security governance in organisations, namely their information security policy review and information security policy awareness programs. When work-from-home arrangements are in place, employees are highly receptive to the information security governance of their organisations. Moreover, it was found that information security policy reviews, which are the regular maintenance of information security policies, and information security policy awareness have a positive impact on the compliance behaviour of employees. This means that employees who are working from home are more likely to comply with information security policies in their organisations if those policies are updated regularly and have policy awareness and training programs in place.

Furthermore, the study found that technostress negatively impacts compliance with information security policies. When ICTs disrupt employees' time schedules and when they have to adapt to new technologies, they are less likely to comply with information security policies. This suggests that techno-invasion is a techno-stressor which has a significant impact on the compliance behaviour employees.

Whilst the initial findings regarding the hypotheses developed in this study are significant in the context of compliance behaviour, this study also made other significant findings, potentially increasing the theoretical and practical implications of this study. The additional findings are discussed below.

5.8. Additional findings

Additionally, it was found that information security governance aspects, such as security policy awareness and security policy review processes in organisations, can be used as a mediator in understanding the impact of work from home on compliance. The findings suggest that when employees are working from home, they are motivated by the information security programs existing in their organisations to comply with information security policies.

Whilst the moderating variables were not shown to be statistically significant in the initial findings, the analysis of the moderation variables showed that telecommuting intensity displays a positive slope in the relationship between technostress and compliance, suggesting that the higher the telecommuting intensity, the higher the technostress, which consequently impacts compliance behaviour negatively. It was found that the relationship between technostress and telecommuting

intensity is statistically significant, and this supports what is known about common work-from-home setups and invasive technologies.

Multigroup analysis showed that gender and age have varying impacts on the compliance behaviour of employees. A significant finding was that telecommuting intensity was a moderating variable in the relationship between technostress and information overload and compliance. Furthermore, it was found in the analysis of the measurement model that altruistic fear has an impact on the compliance behaviour of employees. Although this was not hypothesised, studies by other authors support this finding.

A second multigroup analysis of the age subgroup revealed that there are significant differences in the compliance behaviours of employees according to their respective age groups. It has been found that technostress and job insecurity have a negative impact on compliance to information security policies amongst participants aged 35 and above. Also, telecommuting intensity and altruistic fear both have moderating effects on job technostress, information overload and job insecurity respectively among those aged 35 and above. These findings were less evident for participants aged between 18 and 34.

The results of the subgroup analysis show that the results for the initial hypotheses did not give a conclusive answer for all the subgroups in this study. A discussion of the findings follows in the next section.

5.9. Discussion

Analyses of the measurement model and the structural model assessment were presented in Sections 5.3 and 5.4, and the results of the study were established in Sections5.6, 5.7 and 5.8. The findings were significant in the context of information security policy compliance and information security for the period since the start of the COVID-19 pandemic. The findings yielded some significant results in terms of the hypotheses, and these were supported by literature; H1, H2, H6 and H9a and H9b were supported.

Previous studies concur with the findings of H9a and H9b; they have shown that employees working in organisations with a level of information security governance (policy awareness and policy review) are likely to comply with information security policies. Independent studies have stated that employees are likely to feel duty-bound to comply with information security policies when they see an effort from their organisations to ensure awareness and when organisational practices are evident (Daud et al., 2018; Safa et al., 2016) and when their organisations build an organisational and information security culture (Solomon & Brown, 2021).

Employees, who are working from home, are especially receptive to awareness and review measures inside organisations; this may be because they are aware of the increase in cyberattack attempts targeting employees working remotely and how detrimental these are. A study unrelated to cybersecurity showed that remote work has a positive impact on the satisfaction of employees (Schall, 2019). This supports the findings of H1 and H2 as job satisfaction may translate into employees buying into information security rules and procedures.

Previous studies have shown that technostress has a negative impact on the compliance behaviour of employees (Hwang et al., 2021; Nasirpouri Shadbad & Biros, 2020a). This agrees with the findings of

H6; essentially, technostress is said to cause indecisiveness and a level of frustration in employees, may cause them not to comply with existing information security policies.

Of the hypotheses not supported but conditionally supported by the moderation analysis and multigroup analysis, previous studies in contexts unrelated to cybersecurity but focussing on telecommuting intensity and fear have shown that the moderators used in this study do *not* have an impact on desirable behaviour in organisations when looking at productivity and commitment (Alfanza, 2021; Nagata et al., 2021; Nyaanga, 2012). Hence these contradict the tentative findings of H3 and H4 from the moderation analysis and multigroup analysis. However, it is important to note that these published studies on telecommuting intensity were conducted in contexts unrelated to information security and looked at telecommuting intensity in the context of work engagement, work balance, job satisfaction, productivity and commitment.

It has been shown by Trang and Nastjuk (2021) that information overload has a negative impact on compliance behaviour which contradicts the findings of H5. However, this study was not conducted in the African context and the model measured 'time constraint' to understand information overload. Furthermore, information overload may be better understood if studies take into consideration subgroups - the geographical location of participants, ages of participants and the genders of participants (Wu & Zheng, 2021).

H7 was supported by studies that looked at the positive impact of job insecurity on behaviour pertaining to productivity and performance in organisations (Probst et al., 2007; Staufenbiel & Kö Nig, 2010). Another study, however, showed that job insecurity negatively impacts the commitment of employees as well as the feeling of attachment of employees to organisations (van Zyl et al., 2013). Hence there have been mixed results with regards to the support for the findings H7. While it has been reported that job insecurity makes the insider threat a real cybersecurity threat, but there are few studies conducted on the related but different issue of on job insecurity and information security-related behaviour (compliance). It is important to note that the participants in this study did not feel that their jobs were at risk.

A recent study contradicts the findings of H8, although, in the context unrelated to information security, it shows that altruistic fear has a negative impact on the emotions of individuals (Sloan et al., 2021). The link between emotions and information security behaviour has been drawn in information security research (Boss et al., 2015); thus, the study by Sloan et al. (2021) is relevant in aiding the understanding of this hypothesis.

5.10. Summary

The assessment of the structural model and the measurement of the model yielded satisfactory results in that all construct items passed the validity and reliability assessments. Importantly, the structural assessment, using the R2 measure of fit, indicated that the dependent variable(s) and the linear model have a satisfactory relationship.

Statistical findings from the hypotheses tested showed that specific COVID-19 pandemic-induced contextual factors have some level of impact on the compliance behaviour of employees. Findings show that aspects of information security governance such as security policy awareness and security policy reviews can be a mediator in understanding the relationship telecommuting and compliance behaviour. It was found that telecommuting has a positive impact on employees' perception of policy awareness and policy reviews in the workplace, indicating that the telecommuting norm influences

organisational norms. Findings show that technostress has a negative impact on compliance behaviour.

While some hypotheses were not supported, a further analysis using the multigroup analysis of the age and gender subgroups showed that COVID-19 pandemic-induced contextual factors have varying impacts on compliance behaviour depending on age and gender.

Findings in this study were supported by studies conducted in various contexts; hypotheses not supported were often not widely utilised in the area of cybersecurity, creating opportunities for future research, which will be discussed below.

6. Conclusion, implications, recommendations, and future research

The study had three research questions, the primary one being how COVID-19 pandemic-induced contextual factors influence information security compliance behaviour among employees in organisations with information security policies. For the main research question, the data collected and analysed indicated that some COVID-19 pandemic-induced contextual factors have an impact on compliance behaviour. Furthermore, the data showed that telecommuting influences security policies and procedures of organisations and that the organisational security policies and procedures influence compliance of employees answering the secondary research questions.

This study thus ends by looking at the theoretical implications, practical implications, future research opportunities and a conclusion to the research study.

6.1. Theoretical implications

This study has three theoretical implications. First, the conceptual model in this study and its constructs have been measured and assessed. This creates an opportunity for future researchers to build on this work and to extend our communal understanding of COVID-19 induced contextual factors by applying versions of the model in other contexts. Our conceptual model has not previously been used to understand compliance behaviour evident since the start of the COVID-19 pandemic in a quantitative study using PLS-SEM, so this creates new opportunities for researchers seeking to understand cybersecurity in this time frame. This study conceptualises some COVID-19 pandemic-induced contextual factors, namely, telecommuting, technostress, information overload, job insecurity and altruistic fear, with the intention of understanding their impact on compliance behaviour. COVID-19 and related pandemics are expected to be with us for many years to come and some, if not all, of the contextual factors identified are expected to have an impact on the information security compliance behaviour of employees, especially employees who work from home in some capacity.

Our study extends the focus of studies on compliance behaviour in the workplace by focusing on telecommuting holistically, taking telecommuting intensity into consideration and finally, using telecommuting intensity as a moderator.

Finally, the study contributes to work that has previously been done relating organisational factors to information security governance, specifically, information security policy awareness and information security policy reviews. It provides an understanding of the impact of organisational factors on compliance behaviour. This study investigated the impact that the telecommuting norm has on organisational norms.

6.2. Practical implications

The findings in this study have several practical implications. Since employees working in organisations with work-from-home arrangements are positive about information security rules and procedures, organisations should increase policy awareness programmes and measures to update information security policies.

Employees working from home are highly dependent on competent information security management measures in their organisations. Hence, it is prudent that organisations ensure that all information security measures are fully functional.

Employees feel that technologies are extremely invasive, hence organisations are advised to assist employees working from home to create a heathy and productive work environment. It is said that work body posture and workplace design can reduce technostress; thus, it is advised that organisations embrace ergonomics (Kivimäki, 2022; Mcdonald et al., 2022).

6.3. Recommendations and future research

Future research could look at the impact of COVID-19 pandemic-induced contextual factors on different subgroups, categorised by gender and age, using a significant sample for each of these sub-populations. Different countries have different levels of awareness to cybersecurity and exposures to cyberattack attempts, for example, awareness of cybersecurity threats is much lower in developing countries than in more developed countries. Therefore, it would also be beneficial to take the geographical location of participants into consideration; perhaps a comparative geographical study will give researchers a good understanding of the impact of COVID-19 on cybersecurity.

Furthermore, it would be beneficial to look at the impact of specific COVID-19 pandemic-induced contextual factors on the compliance behaviour of students, many of whom are studying in a hybrid setting. The study reported on here only looked at compliance behaviour in the workplace and this creates a gap. Finally, a larger sample would be recommended. This study had a total number of 298 and whilst this is a sufficient sample for a study using PLS-SEM analysis, a larger sample would be beneficial, especially when the aim is to conduct further multigroup analysis.

6.4. Conclusion

This study looked at the impact of COVID-19 pandemic-induced contextual factors on compliance behaviour, specifically telecommuting, included telecommuting intensity, information overload, technostress, job insecurity and altruistic fear. The study examined the influence of information security rules and procedures within organisations, as well as the impact of telecommuting on these factors, and further explored their effects on employees' compliance behaviour.

Since the pandemic cybercriminals have taken advantage of COVID-19 pandemic-induced contextual factors. Work from home has been the most significant change since the pandemic and it has come with many challenges for organisations. However, working from home is not the only COVID-19 pandemic-induced factor that has boosted the resolve of cybercriminals, the COVID-19 pandemic came with an increase in information overload, technostress, job insecurity and altruistic fear, and these factors have all influenced on how employees behaved.

Using survey questionnaires, data was collected from 298 respondents working in South African organisations that had information security policies and then a quantitative analysis was conducted using PLS-SEM. A measurement of the conceptual model was carried out to test the validity and reliability of the construct items and this was followed by an assessment of the structural model to evaluate the model’s strength. The hypotheses test was conducted using the bootstrapping method with a subsample of 5000, results were able to establish the negative impact of technostress on the compliance behaviour of employees.

The study reveals several key findings. Firstly, telecommuting has a positive impact on aspects of information security governance such as information security policy reviews and awareness programs within organisations. Employees working from home are very willing to cooperate regarding information security governance in their organisations.

Additionally, the study highlights the significance of information security policy reviews and awareness programs in influencing employees' compliance behaviour. When organisations update their information security policies and implement awareness and training programs, employees working from home are more likely to comply with information security policies.

Moreover, the study identifies technostress as a negative factor affecting compliance with information security policies in organisations. Specifically, when employees experience disruptions to their schedules and face challenges adapting to new technologies, their compliance with information security policies decreases. Techno-invasion emerges as a significant stressor impacting employees' compliance behaviour.

To the researcher’s best knowledge, no other study has been conducted on this phenomenon using the combination of constructs (Policy Review, Policy Awareness, Telecommuting Norm, Job Insecurity, Technostress, Information Overload and Altruistic Fear) and the methods used in the collection of the data and analysis of the study. This study has theoretical and implications and presents opportunities for researchers aiming to extend the body of knowledge on compliance behaviour and related topics.

7. References

Åborg, C., & Fernström, E. (2002). Telework-Work Environment and Well Being. A Longitudinal Study.

Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research*, *11*(4), 1401-1407.

Addae, J. A., Simpson, G., & Ampong, G. O. A. (2019). Factors influencing information security policy compliance behavior. *Proceedings - 2019 International Conference on Cyber Security and Internet of Things, ICSIoT 2019*, 43–47. https://doi.org/10.1109/ICSIOT47925.2019.00015

Agbodzie, E. (2020). *Telecommuting*.

Aguirre-Urreta, M. I., Marakas, G. M., & Ellis, M. E. (2013). Measurement of Composite Reliability in Research Using Partial Least Squares: Some Issues and an Alternative Approach.

Aimran, A. N., Mohamad, W., Bin, A., & Afthanorhan, W. (2008). A Comparison Of Partial Least Square Structural Equation Modeling (PLS-SEM) and Covariance Based Structural Equation Modeling (CB-SEM) for Confirmatory Factor Analysis. *Certified International Journal of Engineering Science and Innovative Technology (IJESIT*, *9001*(5).

Alfanza, Ma. T. (2021). Telecommuting Intensity in the Context of COVID-19 Pandemic: Job Performance and Work-Life Balance. *Economics and Business*, *35*(1), 107–116. https://doi.org/10.2478/EB-2021-0007

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers and Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Aljohani, H. (2021). Cyber security threats during the pandemic. www.jcsronline.com

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: a higher education case study. *Information & Computer Security*, *26*(1), 91–108. https://doi.org/10.1108/ICS-09-2016-0073

Alsmadi, I., Burdwell, R., Aleroud, A., Wahbeh, A., Al-Qudah, M., & Al-Omari, A. (2018). Introduction to Information Security. In *Practical Information Security* (pp. 1–16). Springer International Publishing. https://doi.org/10.1007/978-3-319-72119-4_1

Al-Tabash, K., & Happa, J. (2018). Insider-threat detection using Gaussian Mixture Models and Sensitivity Profiles. *Computers & Security*, *77*, 838–859. https://doi.org/10.1016/J.COSE.2018.03.006

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020a). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, *104*, 106184. https://doi.org/10.1016/j.chb.2019.106184

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020b). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, *104*, 106184. https://doi.org/10.1016/j.chb.2019.106184

Anand, S., & Chakravarty, A. (2020). *Cyber Criminals Using COVID-19 Fears to Increase Malicious Online Activity: What You Should Know* . https://www.jdsupra.com/legalnews/cyber-criminals-using-covid-19-fears-to-82090/

Angraini, Alinda Alias, R., & Okfalisa. (2019). Information Security Policy Compliance: Systematic Literature Review. *Procedia Computer Science*, *161*, 1216–1224. https://doi.org/10.1016/j.procs.2019.11.235

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/J.CHB.2016.12.040
Arduin, P. E. (2020). To click or not to click? Deciding to trust or distrust phishing emails. In Decision Support Systems X: Cognitive Decision Support Systems and Technologies: 6th International Conference on Decision Support System Technology, ICDSST 2020, Zaragoza, Spain, May 27–29, 2020, Proceedings 6 (pp. 73-85). Springer International Publishing.
Asmundson, G. J. G., & Taylor, S. (2020). Coronaphobia: Fear and the 2019-nCoV outbreak. *Journal of Anxiety Disorders*, *70*, 102196. https://doi.org/10.1016/J.JANXDIS.2020.102196
Auriacombe, C. J. (2007). *DATA ANALYSIS IN QUANTITATIVE RESEARCH*. https://www.researchgate.net/publication/325780634
Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on Information security policies compliance attitudes. *Information & Computer Security*, *25*(4), 421–436. https://doi.org/10.1108/ICS-11-2016-0089
Bambale, A. (2014). Research Methodological Techniques as a Model for Quantitative Studies in Social Sciences. *British Journal of Economics, Management & Trade*, *4*(6), 862–879. https://doi.org/10.9734/bjemt/2014/7665
Bansal, G., & Shin, S. il. (2016). Interaction Effect of Gender and Neutralization Techniques on Information Security Policy Compliance: An Ethical Perspective. 1.
Barman, S. (2008). *Writing Information Security Policies]*. www.newriders.com
Barnes, S. J. (2020). Information management research and practice in the post-COVID-19 world. *International Journal of Information Management*, *55*, 102175. https://doi.org/10.1016/J.IJINFOMGT.2020.102175
Bartholomew, D. J. (1993). Estimating Relationships between Latent Variables. *Sankhyā: The Indian Journal of Statistics, Series A*. https://www.jstor.org/stable/25050951?seq=1
Bawden, D., & Robinson, L. (2021). Information Overload: An Overview. *Oxford Encyclopedia of Political Decision Making*. https://doi.org/10.1093/ACREFORE/9780190228637.013.1360
Bell, J., & Waters, S. (2018). Ebook: doing your research project: a guide for first-time researchers. McGraw-hill education (UK).
Bermes, A. (2021). Information overload and fake news sharing: A transactional stress perspective exploring the mitigating role of consumers' resilience during COVID-19. *Journal of Retailing and Consumer Services*, *61*, 102555. https://doi.org/10.1016/J.JRETCONSER.2021.102555
Bertram, D. (2007). Likert scales. *Retrieved November*, *2*(10), 1-10.
Binder, C. (2020). Coronavirus Fears And Macroeconomic Expectations. *Review of Economics and Statistics*, *102*(4), 721-730.
Blanuša, J., Barzut, V., & Knežević, J. (2021). Intolerance of Uncertainty and Fear of COVID-19 Moderating Role in Relationship Between Job Insecurity and Work-Related Distress in the Republic of Serbia. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/FPSYG.2021.647972
Borkovich, D., & Middle, G. (2018). Information overload revisited: infinite organizational threats. *Issues Info Sys*, *19*(4), 150-161.
Borkovich, D. J., & Skovira, R. J. (2020a). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, *21*(4).
Borkovich, D. J., & Skovira, R. J. (2020b). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, *21*(4).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly*, *39*(4), 837-864.
Box, D., & Pottas, D. (2013). Improving information security behaviour in the healthcare context. *Procedia Technology*, *9*, 1093–1103. https://doi.org/10.1016/j.protcy.2013.12.122
Brands, K. (2021). *Cybersecurity from Within*. https://sfmagazine.com/post-entry/may-2021-cybersecurity-from-within/
Brivio, E., Gaudioso, F., Vergine, I., Mirizzi, C. R., Reina, C., Stellari, A., & Galimberti, C. (2018). Preventing Technostress Through Positive Technology. *Frontiers in Psychology*, *9*(DEC), 2569. https://doi.org/10.3389/FPSYG.2018.02569
Brown, A. (2020). Why Are Non-malicious Employees Non-Compliant: Guidance for Identifying Employee Negligence and Implementing Information Security Policies to Reduce Employees Inadvertently Becoming Insider Threats (Doctoral dissertation, Utica College).
Bruce, N., Pope, D., & Stanistreet, D. (2008). Quantitative Methods for Health Research A Practical Interactive Guide to Epidemiology and Statistics Second Edition. http://www.wiley.com/go/permissions.
Byrne, U. (2005). *Work-life balance Why are we talking about it at all? 22*(1), 53–59. https://doi.org/10.1177/0266382105052268
Carlson, K. D., & Herdman, A. O. (2012). Understanding the Impact of Convergent Validity on Research Results. *Organizational Research Methods*, *15*(1), 17–32. https://doi.org/10.1177/1094428110392383
Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111–1126. https://doi.org/10.1080/07036337.2020.1853122
Carroll, N., & Conboy, K. (2020). Normalising the "new normal": Changing tech-driven work practices under pandemic time pressure. *International Journal of Information Management*, *55*, 102186. https://doi.org/10.1016/j.ijinfomgt.2020.102186
Chapman, P. (2021). Defending against insider threats with network security's eighth layer. *Computer Fraud and Security*, *2021*(3), 8–13. https://doi.org/10.1016/S1361-3723(21)00029-4
Cheah, J. H., Sarstedt, M., Ringle, C. M., Ramayah, T., & Ting, H. (2018). Convergent validity assessment of formatively measured constructs in PLS-SEM: On using single-item versus multi-item measures in redundancy analyses. *International Journal of Contemporary Hospitality Management*, *30*(11), 3192–3210. https://doi.org/10.1108/IJCHM-10-2017-0649/FULL/XML
Cheung, G. W., & Wang, C. (2017). Current Approaches for Assessing Convergent and Discriminant Validity with SEM: Issues and Solutions. *Https://Doi.Org/10.5465/AMBPP.2017.12706abstract*, *2017*(1), 12706. https://doi.org/10.5465/AMBPP.2017.12706ABSTRACT
Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155
Coles-Kemp, L., & Theoharidou, M. (2010). Insider threat and information security management. *Advances in Information Security*, *49*, 45–71. https://doi.org/10.1007/978-1-4419-7133-3_3
Collins, E., Hutzler, R., & Regne, A. (2020). *Global Lockdown: International Jurisdictions Extend COVID-19 Stay-Home Orders*. https://www.jdsupra.com/legalnews/global-lockdown-international-24216/
Cowles, M., & Davis, C. (1982). *On the Origins of the .05 Level of Statistical Significance*. http://www2.psych.ubc.ca/~schaller/528Readings/CowlesDavis1982.pdf

Creswell, J. W. (2008). Research Design (3rd ed.). https://www.bookmall.co.za/products/research-design-676834?gclid=Cj0KCQjw6-SDBhCMARIsAGbI7UitExG3AqGNTjnbPIbDK1nTt8tlo5ybqMxsexaXtgK6qAfwpklCnNIaAt6_EALw_wcB
Creswell, J. W., Hanson, W. E., Clark, V. L. P., & Morales, A. (2007). *Qualitative Research Designs: Selection and Implementation*. https://doi.org/10.1177/0011000006287390
Crosman. (2020). Data security lapses surge in work-from-home era. American Banker.
Crossland, G., Ertan, A., & Holloway, R. (2021). The Impact of Pandemic-Driven Remote Working on Employee Wellbeing, the Psychological Contract and Cyber Security Remote Working and (In)Security.
Cunliffe, A. L. (2011). *Crafting Qualitative Research: Morgan and Smircich 30 Years On*. https://doi.org/10.1177/1094428110373658
da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136
Dash, G., & Paul, J. (2021a). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, *173*, 121092. https://doi.org/10.1016/J.TECHFORE.2021.121092
Dash, G., & Paul, J. (2021b). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, *173*, 121092. https://doi.org/10.1016/J.TECHFORE.2021.121092
Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? http://www.ijbs.unimas.my/images/repository/pdf/Vol19-no1-paper11.pdf
de Bruin, K., de Haan, Y., Vliegenthart, R., Kruikemeier, S., & Boukes, M. (2021). News Avoidance during the Covid-19 Crisis: Understanding Information Overload. *Https://Doi.Org/10.1080/21670811.2021.1957967*, *9*(9), 1394–1410. https://doi.org/10.1080/21670811.2021.1957967
De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*, 102171. https://doi.org/10.1016/J.IJINFOMGT.2020.102171
de Schrijver, S., & van Loon, J. (2021). *The Upcoming Changes To The EU's Cybersecurity Framework*. https://www.mondaq.com/security/1082026/the-upcoming-changes-to-the-eu39s-cybersecurity-framework
de Witte, H. (2010). Job Insecurity and Psychological Well-being: Review of the Literature and Exploration of Some Unresolved Issues. *Organizational Psychology*, *8*(2), 155–177. https://doi.org/10.1080/135943299398302
deMarrais, K., & Lapan, S. (2003). *Qualitative Interview Studies: Learning Through Experience*. 67–84. https://doi.org/10.4324/9781410609373-8
Desolda, G., di Bari Aldo Moro LAUREN FERRO, U. S., Marrella, A., Catarci, T., Francesca Costabile, M., & di Bari Aldo Moro, U. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review. *Human Factors in Phishing Attacks: A Systematic Literature Review*. *ACM Comput. Surv*, *54*. https://doi.org/10.1145/3469886
De Souzabido, D., & Da Silva, D. (2019). SMARTPLS 3: SPECIFICATION, ESTIMATION, EVALUATION AND REPORTING. *Administração: Ensino e Pesquisa–RAEP*, *20*(2), 465-514.

Dewi, K., & Monalisa, M. (2016). Effect of Corporate Social Responsibility Disclosure on Financial Performance with Audit Quality as a Moderating Variable. *Binus Business Review*, *7*(2), 149–155. https://doi.org/10.21512/BBR.V7I2.1687
Drakulich, K. M. (2015). Concerns for Self or Family? Sources of and Responses to Altruistic Fear. *Journal of Interpersonal Violence*, *30*(7), 1168–1207. https://doi.org/10.1177/0886260514539842
Dupuis, M., & Khadeer, S. (2016). Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat. https://doi.org/10.1145/2978178.2978185
Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). Cyber attacks in the era of covid-19 and possible solution domains.
Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–1168. https://doi.org/10.1111/J.1083-6101.2007.00367.X
Etikan, I., Abubakar Musa, S., & Sunusi Alkassim, R. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11
Fan, J., & Smith, A. P. (2021). Information Overload, Wellbeing and COVID-19: A Survey in China. *Behavioral Sciences 2021, Vol. 11, Page 62*, *11*(5), 62. https://doi.org/10.3390/BS11050062
Fay, M. P., & Proschan, M. A. (2010). Wilcoxon-Mann-Whitney or t-test? On assumptions for hypothesis tests and multiple interpretations of decision rules. *Statistics Surveys*, *4*, 1. https://doi.org/10.1214/09-SS051
Ferketich, S. (1990). Internal consistency estimates of reliability. *Research in Nursing & Health*, *13*(6), 437–440. https://doi.org/10.1002/NUR.4770130612
Fischer, T., Pehböck, A., & Riedl, R. (2019). Is the Technostress Creators Inventory Still an Up-To-Date Measurement Instrument? Results of a Large-Scale Interview Study. https://www.nytimes.com/topic/subject/cyberbullying
Fisher, M. J., & Marshall, A. P. (2009). Understanding descriptive statistics. *Australian Critical Care*, *22*(2), 93–97. https://doi.org/10.1016/J.AUCC.2008.11.003
Flannelly, L. T., Flannelly, K. J., & Jankowski, K. R. B. (2014). Independent, Dependent, and Other Variables in Healthcare and Chaplaincy Research. *Journal of Health Care Chaplaincy*, *20*(4), 161–170. https://doi.org/10.1080/08854726.2014.959374
Flowerday, S. v., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers and Security*, *61*, 169–183. https://doi.org/10.1016/j.cose.2016.06.002
Fonner, K. L., & Roloff, M. E. (2010). Why Teleworkers are More Satisfied with Their Jobs than are Office-Based Workers: When Less Contact is Beneficial. https://www.interruptions.net/literature/Fonner-JApplCommRes10.pdf
Fontanilla, M. v. (2021). *Cybercrime pandemic*. www.eubios.info
Franke, G., & Sarstedt, M. (2019). Heuristics versus statistics in discriminant validity testing: a comparison of four procedures. *Internet Research*, *29*(3), 430–447. https://doi.org/10.1108/INTR-12-2017-0515/FULL/PDF
Furnell, S., & Shah, J. N. (2020). Home working and cyber security – an outbreak of unpreparedness? *Computer Fraud and Security*, *2020*(8), 6–12. https://doi.org/10.1016/S1361-3723(20)30084-1

Gajendran, R. S., & Harrison, D. A. (2007). The Good, the Bad, and the Unknown About Telecommuting: Meta-Analysis of Psychological Mediators and Individual Consequences. https://doi.org/10.1037/0021-9010.92.6.1524
Gasparro, R., Scandurra, C., Maldonato, N. M., Dolce, P., Bochicchio, V., Valletta, A., Sammartino, G., Sammartino, P., Mariniello, M., Lauro, A. E. di, & Marenzi, G. (2020). Perceived Job Insecurity and Depressive Symptoms among Italian Dentists: The Moderating Role of Fear of COVID-19. *International Journal of Environmental Research and Public Health 2020, Vol. 17, Page 5338*, *17*(15), 5338. https://doi.org/10.3390/IJERPH17155338
Gelman, A., & Stern, H. (2012). The Difference Between "Significant" and "Not Significant" is not Itself Statistically Significant. https://doi.org/10.1198/000313006X152649
Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 1–20. https://doi.org/10.1057/s41284-021-00286-2
Gerard, J., & Caillier, J. G. (2012). Satisfaction With Work-Life Benefits and Organizational Commitment/Job Involvement: Is There a Connection? *Review of Public Personnel Administration*, *33*(4), 340–364. https://doi.org/10.1177/0734371X12443266
Ghislieri, C., Molino, M., Dolce, V., Sanseverino, D., & Presutti, M. (2021). Work-family conflict during the Covid-19 pandemic: teleworking of administrative and technical staff in healthcare. An Italian study. *La Medicina Del Lavoro*, *112*(3), 229. https://doi.org/10.23749/MDL.V112I3.11227
Golden, T. D., Veiga, J. F., & Dino, R. N. (2008). The Impact of Professional Isolation on Teleworker Job Performance and Turnover Intentions: Does Time Spent Teleworking, Interacting Face-to-Face, or Having Access to Communication-Enhancing Technology Matter? *Journal of Applied Psychology*, *93*(6), 1412–1421. https://doi.org/10.1037/A0012722
Götz, O., Liehr-Gobbers, K., & Krafft, M. (2010). Evaluation of Structural Equation Models Using the Partial Least Squares (PLS) Approach. *Handbook of Partial Least Squares*, 691–711. https://doi.org/10.1007/978-3-540-32827-8_30
Greenhalgh, L., & Rosenblatt, Z. (1984). Job Insecurity: Toward Conceptual Clarity. *The Academy of Management Review*, *9*(3), 438. https://doi.org/10.2307/258284
Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *IEEE Security and Privacy*, *6*(1), 61–64. https://doi.org/10.1109/MSP.2008.8
Guhr, N., Lebek, B., & Breitner, M. H. (2018). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. https://doi.org/10.1111/isj.12202
Hair, J. F. Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis : a global perspective. In *Pearson Education, Inc.* Pearson Education,.
Hair, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107. https://doi.org/10.1504/IJMDA.2017.087624
Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). Journal of Marketing Theory and Practice PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202
Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014a). *Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research*. https://doi.org/10.1108/EBR-10-2013-0128

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014b). *Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research*. https://doi.org/10.1108/EBR-10-2013-0128
Hair, J. F., Sarstedt, M., & Ringle, C. M. (2019). Rethinking some of the rethinking of partial least squares. *European Journal of Marketing*, *53*(4), 566–584. https://doi.org/10.1108/EJM-10-2018-0665/FULL/PDF
Hamid, H. A., Mohd-Yusof, M., Ridzwan, N., & Dali, S. M. (2017). *Security Compliance Behaviour of SaaS Cloud Users: A Pilot Study*. https://doi.org/10.3923/jeasci.2017.4150.4155
Handy, S., & Mokhtarian, P. (1996). *The Future of Telecommuting*. https://escholarship.org/content/qt5nm777c1/qt5nm777c1.pdf
Harris, K. J., Harris, R. B., Valle, M., Carlson, J., Carlson, D. S., Zivnuska, S., & Wiley, B. (2022). Technostress and the entitled employee: impacts on work and family. *Information Technology and People*, *35*(3), 1073–1095. https://doi.org/10.1108/ITP-07-2019-0348/FULL/PDF
Hassandoust, F., & Techatassanasoontorn, A. A. (2020). Understanding users' information security awareness and intentions: A full nomology of protection motivation theory. In *Cyber Influence and Cognitive Threats* (pp. 129–143). Elsevier. https://doi.org/10.1016/B978-0-12-819204-7.00007-5
Henseler, J. (2007). A New and Simple Approach to Multi-Group Analysis in Partial Least Squares Path Modeling. http://hdl.handle.net/2066/160875
Henseler, J. (2012). PLS-MGA: A Non-Parametric Approach to Partial Least Squares-based Multi-Group Analysis. *Studies in Classification, Data Analysis, and Knowledge Organization*, 495–501. https://doi.org/10.1007/978-3-642-24466-7_50
Hill, R., & Hamilton, W. P. (1998). WHAT SAMPLE SIZE is "ENOUGH" in INTERNET SURVEY RESEARCH?
Hilmer, T., & Futcher, L. (2019). A strategy for improving the maturity levels of IT Service Management in Higher Education Institutions in South Africa.
Holden, M. T., & Lynch, P. (2006). Choosing the Appropriate Methodology: Understanding Research Philosophy. *The Marketing Review*, *4*(4), 397–409. https://doi.org/10.1362/1469347042772428
Holliss, F. (2021). Working from Home. *Built Environment*, *47*(3), 367–379. https://doi.org/10.2148/BENV.47.3.367
Höne, K., & Eloff, J. H. P. (2002). Information security policy - What do international information security standards say? In *Computers and Security* (Vol. 21, Issue 5, pp. 402–409). Elsevier Ltd. https://doi.org/10.1016/S0167-4048(02)00504-7
Hoog, N. de, Stroebe, W., & Wit, J. B. F. de. (2008). The processing of fear-arousing communications: How biased processing leads to persuasion. *Https://Doi.Org/10.1080/15534510802185836*, *3*(2), 84–113. https://doi.org/10.1080/15534510802185836
Hooper, V., & Blunt, C. (2019). Factors influencing the information security behaviour of IT employees. *Https://Doi.Org/10.1080/0144929X.2019.1623322*, *39*(8), 862–874. https://doi.org/10.1080/0144929X.2019.1623322
Hu, S. C., & Chen, I. C. (2011). Alleviating information overload caused by volumes of numerical web data: The concept and development process. *IET Software*, *5*(5), 445–453. https://doi.org/10.1049/IET-SEN.2010.0099
Hunton, J. E., & Norman, C. S. (2010). The impact of alternative telework arrangements on organizational commitment: Insights from a longitudinal field experiment. *Journal of Information Systems*, *24*(1), 67–90. https://doi.org/10.2308/JIS.2010.24.1.67

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282–293. https://doi.org/10.1016/J.CHB.2017.12.022
Hwang, I., Kim, S., & Rebman, C. (2021). Impact of regulatory focus on security technostress and organizational outcomes: the moderating effect of security technostress inhibitors. https://doi.org/10.1108/ITP-05-2019-0239
Ichimura, T., Uemoto, T., & Kamada, S. (2017). Altruistic behaviours-based recommendation system of tourist information from smartphone application to SNS community. *International Journal of Computational Intelligence Studies*, *6*(4), 270. https://doi.org/10.1504/IJCISTUDIES.2017.089510
Ifinedo, P. (2014). Information Systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79. https://doi.org/10.1016/J.IM.2013.10.001
In, J. (2017). Introduction of a pilot study. *Korean Journal of Anesthesiology*, *70*(6), 601. https://doi.org/10.4097/KJAE.2017.70.6.601
Ingusci, E., Signore, F., Giancaspro, M. L., Manuti, A., Molino, M., Russo, V., Zito, M., & Cortese, C. G. (2021). Workload, Techno Overload, and Behavioral Stress During COVID-19 Emergency: The Role of Job Crafting in Remote Workers. *Frontiers in Psychology*, *12*, 1141. https://doi.org/10.3389/FPSYG.2021.655148/BIBTEX
Iriqat, Y. M., Ahlan, A. R., & Molok, N. N. A. (2019). Information security policy perceived compliance among staff in palestine universities: An empirical pilot study. *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 - Proceedings*, 580–585. https://doi.org/10.1109/JEEIT.2019.8717438
Isaac, S., & Michael, W. B. (1995). *Handbook in research and evaluation: a*. 262. https://books.google.com/books/about/Handbook_in_Research_and_Evaluation.html?id=o5RgQgAACAAJ
Jasgur, C. (2021). COVID-19: Transitioning to the new normal. *Journal of Business Continuity & Emergency Planning*. https://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=f390e176-e27f-4b3a-a43a-21bb73eb02dd%40sessionmgr102
Jeon, S., Son, I., & Han, J. (2020). Exploring the role of intrinsic motivation in ISSP compliance: enterprise digital rights management system case. *Information Technology & People*, *34*(2), 599–616. https://doi.org/10.1108/ITP-05-2018-0256
Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2017). Dispositional and situational factors: influences on information security policy violations. *Https://Doi.Org/10.1057/Ejis.2015.15*, *25*(3), 231–251. https://doi.org/10.1057/EJIS.2015.15
Jun-Hwa, C., Ali Memon, M., & Chuah, F. (2020). *Multigroup Analysis using SmartPLS: Step-by-Step Guidelines for Business Research*. https://doi.org/10.14707/ajbr.200087
Kantor, A. (2021). *Coronavirus triggers epidemic of cyber fraud*. https://www.ft.com/content/30553ae9-cdfd-483c-a1ef-c04e3135f9da
Karlsson, F., Karlsson, M., & Åström, J. (2017). Measuring employees' compliance – the importance of value pluralism. *Information & Computer Security*, *25*(3), 279–299. https://doi.org/10.1108/ICS-11-2016-0084
Kaur, P., Stoltzfus, J., & Yellapu, V. (2018). Descriptive statistics. *International Journal of Academic Medicine*, *4*(1), 60. https://doi.org/10.4103/IJAM.IJAM_7_18
Kautondokwa, P., Ruhwanya, Z., & Ophoff, J. (2021). *Environmental Uncertainty and End-User Security Behaviour: A Study During the COVID-19 Pandemic*. 111–125. https://doi.org/10.1007/978-3-030-80865-5_8

Kim, H. L., & Han, J. (2018). Do employees in a “good” company comply better with information security policy? A corporate social responsibility perspective. *Information Technology & People*, *32*(4), 858–875. https://doi.org/10.1108/ITP-09-2017-0298
Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, *21*(4), 986–1010. https://doi.org/10.1108/JKM-08-2016-0353
Kivimäki, I. (2022). Female remote workers’ technostress - Finnish female knowledge workers’ experiences of daily remote working during the COVID-19 pandemic. https://www.doria.fi/handle/10024/184617
Koh, K., Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2005). Security governance: Its impact on security culture.
Knapp, K. J., & Ferrante, C. J. (2012a). Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations.
Knapp, K. J., & Ferrante, C. J. (2012b). Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations.
Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers and Security*, *28*(7), 493–508. https://doi.org/10.1016/j.cose.2009.07.001
Kot, P. (2022). Technostress and Counterproductive Behaviours in an Organisation. *Technium Social Sciences Journal*, *27*. https://heinonline.org/HOL/Page?handle=hein.journals/techssj27&id=481&div=45&collection=journals
Kroeze, J. H. (2012). *Interpretivism in IS – a Postmodernist (or Postpositivist?) Knowledge Theory*. *1*. http://aisel.aisnet.org/amcis2012/proceedings/PerspectivesIS/7
Kwong, K., & Wong, K. (2013). Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS. *Marketing Bulletin*, *24*. http://marketing-bulletin.massey.ac.nz
Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the paandemic. In *arXiv* (Vol. 105, p. 102248). arXiv. https://doi.org/10.1016/j.cose.2021.102248
Lang, M., Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, J. D. (2016). *The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study*. https://www.researchgate.net/publication/323550750
Lee, G., & Lee, W. J. (2010). Altruistic traits and organizational conditions in helping online. *Computers in Human Behavior*, *26*(6), 1574–1580. https://doi.org/10.1016/J.CHB.2010.06.003
Lee, J., & Han, S. H. (2021). The Future of Service Post-COVID-19 Pandemic, Volume 1 The ICT and Evolution of Work Series Editor: Jungwoo Lee. http://www.springer.com/series/16400
Lewis, R. A. (2013). The Influence of Information Technology on Telework: The Experiences of Teleworkers and Their Non-Teleworking Colleagues in a French Public Administration. *International Journal of Information and Education Technology*. http://www.ijiet.org/papers/229-T1004.pdf
Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019a). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/J.IJINFOMGT.2018.10.017
Li, X., Zhang, S., Wang, C., & Guo, X. (2017). Understanding customers’ compliance behaviour to frontline employees’ fuzzy requests. *Journal of Services Marketing*, *32*(2), 235–246. https://doi.org/10.1108/JSM-03-2016-0122

Li, Y., Pan, T., & Zhang, N. (2019b). From hindrance to challenge: How employees understand and respond to information security policies. *Journal of Enterprise Information Management*, *33*(1), 191–213. https://doi.org/10.1108/JEIM-01-2019-0018
Liu, C., Liang, H., Wang, N., & Xue, Y. (2021). Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender. *Information Technology & People*. https://doi.org/10.1108/ITP-09-2019-0452
Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, *57*(2), 123–146. https://doi.org/10.1109/TPC.2014.2312452
Lueck, M. (2020). GDPR In The New Remote-Working Normal. *Computer Fraud and Security*, *2020*(8), 14–16. https://doi.org/10.1016/S1361-3723(20)30086-5
Mabuza, E. (2020). *Cyber Crimes "On The Rise" During Covid-19 Lockdown, Warn Experts*. https://www.timeslive.co.za/news/south-africa/2020-04-28-7am-cyber-crimes-on-the-rise-during-covid-19-lockdown-warn-experts/
MacKinnon, D. P. (2015). Mediating Variable. *International Encyclopedia of the Social & Behavioral Sciences: Second Edition*, 64–69. https://doi.org/10.1016/B978-0-08-097086-8.44037-7
Madhi, S. A., Kwatra, G., Myers, J. E., Jassat, W., Dhar, N., Mukendi, C. K., Nana, A. J., Blumberg, L., Welch, R., Ngorima-Mabhena, N., & Mutevedzi, P. C. (2022). Population Immunity and Covid-19 Severity with Omicron Variant in South Africa. *The New England Journal of Medicine*. https://doi.org/10.1056/NEJMOA2119658/SUPPL_FILE/NEJMOA2119658_DISCLOSURES.PDF
Malmqvist, J., Hellberg, K., Möllås, G., Rose, R., & Shevlin, M. (2019). Conducting the Pilot Study: A Neglected Part of the Research Process? Methodological Findings Supporting the Importance of Piloting in Qualitative Research Studies. https://doi.org/10.1177/1609406919878341
Matthews, L. (2017). Applying Multigroup Analysis in PLS-SEM: A Step-by-Step Process. *Partial Least Squares Path Modeling: Basic Concepts, Methodological Issues and Applications*, 219–243. https://doi.org/10.1007/978-3-319-64069-3_10
Mcbride, M., Carter, L., & Warkentin, M. (2012). Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies. www.dhs.gov
Mcdonald, K. S., Hite, L. M., & O'connor, K. W. (2022). Developing sustainable careers for remote workers. https://doi.org/10.1080/13678868.2022.2047148
Meilee, C., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *J Med Internet Res 2020;22(9):E23692 Https://Www.Jmir.Org/2020/9/E23692*, *22*(9), e23692. https://doi.org/10.2196/23692
Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to Malware Incident Prevention and Handling.
Meltzer, H., Bebbington, P., Brugha, T., Jenkins, R., Mcmanus, S., & Stansfeld, S. (2009). Job Insecurity, Socio-Economic Circumstances And Depression. https://doi.org/10.1017/S0033291709991802
Memon, M. A., Jun, H. C., Ting, H., & Francis, C. W. (2018). Mediation analysis issues and recommendations. *Journal of Applied Structural Equation Modeling*, *2*(1), i-ix.
Mertens, G., Gerritsen, L., Duijndam, S., Salemink, E., & Engelhard, I. M. (2020). Fear of the coronavirus (COVID-19): Predictors in an online study conducted in March 2020. *Journal of Anxiety Disorders*, *74*, 102258. https://doi.org/10.1016/J.JANXDIS.2020.102258

Michaelides, N. (2021). Remote Working and Cyber Security Literature Review. https://www.researchgate.net/publication/349396561
Mikhalkin, E. N., Tsikh -, A. K., Afthanorhan, A., Liza Ghazali, P., Rashid, N., Ab Hamid, M. R., Sami, W., & Mohmad Sidek, M. H. (2017). Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion. *J. Phys*, *890*, 12163. https://doi.org/10.1088/1742-6596/890/1/012163
Minnaar, A. (2020). 'Gone Phishing': The Cynical And Opportunistic Exploitation Of The Coronavirus Pandemic By Cybercriminals. *Acta Criminologica: African Journal of Criminology & Victimology*. https://journals.co.za/doi/pdf/10.10520/ejc-crim-v33-n3-a3
Mladenović, D., Todua, N., & Pavlović-Höck, N. (2022). The More We Know, the More We Want to Know: Information Overload and Cyberchondria During Covid-19. https://papers.ssrn.com/abstract=4091552
Mohamad, W., Bin, A., & Afthanorhan, W. (2008). A Comparison Of Partial Least Square Structural Equation Modeling (PLS-SEM) and Covariance Based Structural Equation Modeling (CB-SEM) for Confirmatory Factor Analysis. *Certified International Journal of Engineering Science and Innovative Technology (IJESIT)*, *9001*(5), 2319–5967.
Mohammed, M., Sha'aban, A., Jatau, A. I., Yunusa, I., Isa, A. M., Wada, A. S., Obamiro, K., Zainal, H., & Ibrahim, B. (2022). Assessment of COVID-19 Information Overload Among the General Public. *Journal of Racial and Ethnic Health Disparities*, *9*(1), 184–192. https://doi.org/10.1007/S40615-020-00942-0/TABLES/4
Monroe, B. (2020). *Fraud, cybercrime, surging now, AML must later look for launderers hiding in economic recovery, volatility*. https://www.acfcs.org/regional-spotlight-europe-fraud-cybercrime-surging-now-aml-must-later-look-for-launderers-hiding-in-economic-recovery-volatility/
Morin, K. H. (2013). Value of a pilot study. *Journal of Nursing Education*, *52*(10), 547–548. https://doi.org/10.3928/01484834-20130920-10
Mungly, I., Singh, A. M., & Mungly, M. I. (2012). Understanding the Effect of Information Overload on Teleworkers The Effective Management of Information Overload within Shipping Companies in South Africa View project Business Rescue in SA View project. https://www.researchgate.net/publication/263714884
Murphy, C. (2020). *3 ways to pandemic-proof your cyber security*. https://www.ey.com/en_ie/covid-19/3-ways-to-pandemic-proof-your-cyber-security
Mwagwabi, F., & Jiow, J. H. (2021). Compliance with security guidelines in teenagers. *Australasian Journal of Information Systems*, *25*, 1–25. https://doi.org/10.3127/AJIS.V25I0.2953
Nagata, T., Nagata, M., Ikegami, K., Hino, A., Tateishi, S., Tsuji, M., Matsuda, S., Fujino, Y., & Mori, K. (2021). Intensity of Home-Based Telework and Work Engagement During the COVID-19 Pandemic. *Journal of Occupational and Environmental Medicine*, *63*(11), 907. https://doi.org/10.1097/JOM.0000000000002299
Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222
Naik, S. (2021). *SA hospitals under further strain due to increase in cyber attacks*. https://www.iol.co.za/saturday-star/news/sa-hospitals-under-further-strain-due-to-increase-in-cyber-attacks-efb62b96-9170-43e9-b1af-475783472ba9
Nanayakkara, K. A. D. S. A., & Peiris, T. S. G. (2017). Influence of mathematics on academic performance of engineering students: PLS-SEM approach. *COMMUNICATIONS IN STATISTICS: CASE STUDIES*. https://doi.org/10.1080/23737484.2017.1391724

Nasir, A., Nasir, A., Arshah, R. A., & Hamid, M. R. A. (2018). The Significance of Main Constructs of Theory of Planned Behavior in Recent Information Security Policy Compliance Behavior Study: A Comparison among Top Three Behavioral Theories. *International Journal of Engineering & Technology*, *7*(2.29), 737–741. https://doi.org/10.14419/ijet.v7i2.29.14008
Nasirpouri Shadbad, F., & Biros, D. (2020a). Technostress and its influence on employee information security policy compliance. *Information Technology & People*. https://doi.org/10.1108/ITP-09-2020-0610
Nasirpouri Shadbad, F., & Biros, D. (2020b). Technostress and its influence on employee information security policy compliance. *Information Technology & People*. https://doi.org/10.1108/ITP-09-2020-0610
Nurse, J. R., C, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). *An Analysis of New Threats and Risks to Security and Privacy*. http://kar.kent.ac.uk/contact.html
Nyaanga, S. (2012). The Impact of Telecommuting Intensity on Employee Perception Outcomes: Job Satisfaction, Productivity, and Organizational Commitment.
Okereafor, K., & Manny, P. (2020). Understanding cybersecurity challenges of telecommuting and video conferencing applications in the COVID-19 pandemic. *Journal Homepage: http://ijmr. net. in*, *8*(6).
Omar, M. (2015). Insider threats: Detecting and controlling malicious insiders. In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 162-172). IGI Global.
Onder, C. C. (2016). Unfolding of telecommuting's effects in organizations : performance, commitment, and mechanisms of action.
Padilla, G. v. (1984). Technical Notes: Reliability and Validity of the Independent Variable. *Http://Dx.Doi.Org/10.1177/019394598400600121*, *6*(1), 138–140. https://doi.org/10.1177/019394598400600121
Patton, M. Q. (2002). Two Decades of Developments in Qualitative Inquiry: A Personal, Experiential Perspective. *Http://Dx.Doi.Org/10.1177/147332500200100363 6*, *1*(3), 261–283. https://doi.org/10.1177/147332500200100363 6
Petter, S. (2018a). " haters Gonna hate": PLS and Information Systems research. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(2), 10-13.
Petter, S. (2018b). " haters Gonna hate": PLS and Information Systems research. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(2), 10-13.
Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers and Security*, *23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006
Poulose, S., & Dhal, M. (2020). Role of perceived work–life balance between work overload and career commitment. *Journal of Managerial Psychology*, *35*(3), 169–183. https://doi.org/10.1108/JMP-03-2018-0117/FULL/PDF
Powner, L. C. (2017). Preparing Quantitative Data for Analysis. *Empirical Research and Writing: A Political Science Student's Practical Guide*, 180–205. https://doi.org/10.4135/9781483395906.N8
Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247. https://doi.org/10.1002/itl2.247
Price, J. D. (2014). Abstract Reducing the Risk of a Data Breach Using Effective Compliance Programs.
Probst, T. M., Stewart, S. M., Gruys, M. L., & Tierney, B. W. (2007). Productivity, counterproductivity and creativity: The ups and downs of job insecurity. *Journal of Occupational and Organizational Psychology*, *80*(3), 479–497. https://doi.org/10.1348/096317906X159103

Radzikowski, R. (2020). *Working from Home? Here's Our Security Tips for Remote Work.* https://www.securicy.com/blog/working-secure-while-working-remote/
Ragu-Nathan, T. S., Tarafdar, M., Nathan, R., Ragu-Nathan, B. S., & Tu, Q. (2008). The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation. *Information Systems Research*, *19*(4), 417–433. https://doi.org/10.1287/isre.1070.0165
Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and validation. *Information Systems Research*, *19*(4), 417–433. https://doi.org/10.1287/ISRE.1070.0165
Renaud, K., & Ophoff, J. (2021). *What is Preventing UK SMEs from taking Cyber Security Precautions?* https://www.statista.com/statistics/586565/cyber-essentials-scheme-awareness-by-united-kingdom-uk-businesses/
Richberg, J. (2020). *Pandemic underscores the importance of security, agility for remote work*. https://gcn.com/articles/2020/08/10/secure-agile-telework.aspx
Roos, W., & Van, E. R. (2008). The Relationship Between Employee Motivation. *Job Satisfaction*.
Safa, Nader Sohrabi, Rossouw Von Solms, and Steven Furnell. "Information security policy compliance model in organizations." *computers & security* 56 (2016): 70-82.
Samek Lodovici, M. (2021). The impact of teleworking and digital work on workers and society.
Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* (8th ed.). Pearson Education Limited. www.pearson.com/uk
Saunders, M., & Tosey, P. (2013). *The Layers of Research Design*.
Scarfone, K., Greene, J., & Souppaya, M. (2020). *Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions*. https://csrc.nist.gov/publications/detail/itl-bulletin/2020/03/security-for-enterprise-telework-remote-access-and-byod/final
Schall, M. A. (2019). The relationship between remote work and job satisfaction: The mediating roles of perceived autonomy, work-family conflict, and telecommuting intensity(Doctoral dissertation, San Jose State University).
Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. *Information & Computer Security*, *28*(2), 261–292. https://doi.org/10.1108/ICS-02-2019-0033
Schmidt, F. L., Viswesvaran, C., & Ones, D. S. (2000). Reliability Is Not Validity And Validity Is Not Reliability. *Personnel Psychology*, *53*(4), 901–912. https://doi.org/10.1111/J.1744-6570.2000.TB02422.X
Schmitt, J. B., Breuer, J., & Wulf, T. (2021). From cognitive overload to digital detox: Psychological implications of telework during the COVID-19 pandemic. *Computers in Human Behavior*, *124*, 106899. https://doi.org/10.1016/J.CHB.2021.106899
Segal, E. (2021). *Survey Finds Email Fatigue Could Lead 38% Of Workers To Quit Their Jobs*. https://www.forbes.com/sites/edwardsegal/2021/04/21/survey-finds-email-fatigue-could-lead-38-of-workers-to-quit-their-jobs/?sh=4e03dace25d9
Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. john wiley & sons.
Singh, A. N., & Gupta, M. P. (2013). *Identifying factors of "organizational information security management."* https://doi.org/10.1108/JEIM-07-2013-0052
Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion are employees putting your company at risk by not following information security policies? In *Communications of the*

ACM (Vol. 52, Issue 12, pp. 145–147). ACM PUB27 New York, NY, USA . https://doi.org/10.1145/1610252.1610289
Sloan, M. M., Haner, M., Graham, A., Cullen, F. T., Pickett, J. T., & Jonson, C. L. (2021). Pandemic emotions: the extent, correlates, and mental health consequences of fear of COVID-19. *Https://Doi.Org/10.1080/02732173.2021.1926380*, *41*(5), 369–386. https://doi.org/10.1080/02732173.2021.1926380
Smit, N. W. H., de Beer, L. T., & Pienaar, J. (2016). Work stressors, job insecurity, union support, job satisfaction and safety outcomes within the iron ore mining environment. *SA Journal of Human Resource Management*, *15*. https://doi.org/10.4102/SAJHRM.V14I1.719
Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *34*(4), 1203-1228.
Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., Magnus väg, O., TeodorSommestad, S., & Bengtsson Johan Bengtsson, J. (2014). *Variables influencing information security policy compliance: a systematic review of quantitative studies*.
Spielman, R. M., Dumper, K., Jenkins, W., Lacombe, A., Lovett, M., & Perlmutter, M. (2014). *Why Is Research Important?* OpenStax.
Spiess, T., Ploder, C., Bernsteiner, R., & Dilger, T. (2021). Techno-stress in the workplace: triggers, outcomes, and coping strategies with a special focus on generational differences. *International Journal of Web Engineering and Technology*, *16*(3), 217–234. https://doi.org/10.1504/IJWET.2021.119875
Spilker, M. (2014). Making Telework Work: The Effect of Telecommuting Intensity on Employee Work Outcomes. *Dissertations*. https://irl.umsl.edu/dissertation/215
Stana, R., & Nicolajsen, H. W. (2021). Sociological Mechanisms Behind ICT-Related Technostress in the Workplace. *Information Technology in Organisations and Societies: Multidisciplinary Perspectives from AI to Technostress*, 85–110. https://doi.org/10.1108/978-1-83909-812-320211004
Stanton, J., Mastrangelo, P., Stam, K., Jolton, J., Stanton, J. M., Mastrangelo, P. R., & Stam, K. R. (2004). *Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices*. *175*. http://aisel.aisnet.org/amcis2004http://aisel.aisnet.org/amcis2004/175
Staufenbiel, T., & Kö Nig, C. J. (2010). A model for the effects of job insecurity on performance, turnover intention, and absenteeism. *Journal of Occupational and Organizational Psychology*, *83*, 101–117. https://doi.org/10.1348/096317908X401912
Stebbins, R. A. (2001). Exploratory research in the social sciences (Vol. 48). Sage.
Stine, R. A. (1995). Graphical interpretation of variance inflation factors. *American Statistician*, *49*(1), 53–56. https://doi.org/10.1080/00031305.1995.10476113
Straub. Detmar W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(2), 147–165. https://doi.org/10.2307/248922
Streukens, S., & Leroi-Werelds, S. (2016). Bootstrapping and PLS-SEM: A step-by-step guide to get more out of your bootstrap results. *European Management Journal*, *34*(6), 618–632. https://doi.org/10.1016/J.EMJ.2016.06.003
Sturgeon, A. (1996). Telework: threats, risks and solutions. *Information Management & Computer Security*, *4*(2), 27–38. https://doi.org/10.1108/09685229610121017
Suárez Álvarez, J., Pedrosa, I., Lozano, L. M., García Cueto, E., Cuesta Izquierdo, M., & Muñiz Fernández, J. (2018). Using reversed items in likert scales: A questionable practice. *Scopus*, *30*(2), 149–158. https://doi.org/10.7334/PSICOTHEMA2018.33

Taghva, M. R. (2021a). The Effect of Security Awareness on Compliance with Security Regulations by Teleworkers in the Period of COVID-19 Epidemic. In *Management Researches* (Vol. 13, Issue 50). https://doi.org/10.22111/JMR.2021.35530.5176
Taghva, M. R. (2021b). The Effect of Security Awareness on Compliance with Security Regulations by Teleworkers in the Period of COVID-19 Epidemic. In *Management Researches* (Vol. 13, Issue 50). https://doi.org/10.22111/JMR.2021.35530.5176
Tanpipat, W., Lim, H. W., & Deng, X. (2021). Implementing Remote Working Policy in Corporate Offices in Thailand: Strategic Facility Management Perspective. *Sustainability 2021, Vol. 13, Page 1284*, *13*(3), 1284. https://doi.org/10.3390/SU13031284
Thiese, M. S., Ronna, B., & Ott, U. (2016). P value interpretations and considerations. *Journal of Thoracic Disease*, *8*(9), E928. https://doi.org/10.21037/JTD.2016.08.16
Tiedens, L. Z., & Linton, S. (1994). Judgment Under Emotional Certainty and Uncertainty: The Effects of Specific Emotions on Information Processing. *Rusting*.
Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers & Security*, *104*, 102222. https://doi.org/10.1016/J.COSE.2021.102222
Turnbull, D., Chugh, R., & Luck, J. (2021). Learning management systems: a review of the research methodology literature in Australia and China. *International Journal of Research and Method in Education*, *44*(2), 164–178. https://doi.org/10.1080/1743727X.2020.1737002
Ullah Khan, H., & Alshare, K. A. (2019). Violators versus non-violators of information security measures in organizations-A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 4–23. https://doi.org/10.1080/10919392.2019.1552743
Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in Information Systems research using Partial Least Squares Structural Equation Modeling in Information Systems Research Using Partial Least Squares Structural Equation Modeling in Information Systems Research Using Partial Least Squares. 11(2), 5–40. https://www.researchgate.net/publication/228467554
van Zyl, L., van Eeden, C., & Rothmann, S. (2013). Job insecurity and the emotional and behavioural consequences thereof. *J.Bus.Manage*, *1*, 44.
vanden Abeele, M. M. P., Antheunis, M. L., Pollmann, M. M. H., Schouten, A. P., Liebrecht, C. C., van der Wijst, J., van Amelsvoort, M. A. A., Bartels, J., Krahmer, E. J., & Maes, F. A. (2018). *Communication Studies Does Facebook Use Predict College Students' Social Capital? A Replication of Ellison, Steinfield, and Lampe's (2007) Study Using the Original and More Recent Measures of Facebook Use and Social Capital*. https://doi.org/10.1080/10510974.2018.1464937
vander Elst, T., de Witte, H., & de Cuyper, N. (2014). The Job Insecurity Scale: A psychometric evaluation across five European countries. *European Journal of Work and Organizational Psychology*, *23*(3), 364–380. https://doi.org/10.1080/1359432X.2012.745989
Vasic, M. (2020). Challenges of teleworking during the COVID-19 pandemic. *Economics in Subotica*, *56*(44), 63–079. https://doi.org/10.5937/AnEkSub2044063V
Vehkalahti, K., Puntanen, S., & Tarkkonen, L. (2006). Estimation of reliability: a better alternative for Cronbach's alpha.
von Solms, R., & von Solms, S. H. (Basie). (2006). Information security governance: Due care. *Computers and Security*, *25*(7), 494–497. https://doi.org/10.1016/j.cose.2006.08.013
Wang, C., Yuan, T., Feng, J., & Peng, X. (2022). How can leaders alleviate employees' workplace anxiety caused by information overload on enterprise social media? Evidence from

Chinese employees. *Information Technology and People*. https://doi.org/10.1108/ITP-01-2021-0097/FULL/PDF
Wang, W., Albert, L., & Sun, Q. (2020). Employee isolation and telecommuter organizational commitment. *Employee Relations: The International Journal*, *42*(3), 609–625. https://doi.org/10.1108/ER-06-2019-0246
Warkentin, M., & Johnston, A. C. (2006). IT Security Governance and Centralized Security Controls. In *Enterprise Information Systems Assurance and System Security* (pp. 16–24). IGI Global. https://doi.org/10.4018/978-1-59140-911-3.ch002
Warkentin, M., & Johnston, A. C. (2008). IT governance and organizational design for security management. *Information security: Policies, processes, and practices*, 46-68.
Warkentin, M., & Willison, R. (2017). Behavioral and policy issues in Information Systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101–105. https://doi.org/10.1057/ejis.2009.12
Warr, M., & Ellison, C. G. (2000a). Rethinking social reactions to crime: Personal and altruistic fear in family households. *American Journal of Sociology*, *10*(3), 551–578. https://doi.org/10.1086/318964
Warr, M., & Ellison, C. G. (2000b). Rethinking social reactions to crime: Personal and altruistic fear in family households. *American Journal of Sociology*, *10*(3), 551–578. https://doi.org/10.1086/318964/0
Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 968–5227. https://doi.org/10.1108/09685220910944722
Westermann, T. (2017). User Acceptance of Mobile Notifications. *T-Labs Series in Telecommunication Services*, 3–6. https://doi.org/10.1007/978-981-10-3851-8_1
Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N., & Yaokumah, W. (2020). The role of norms in information security policy compliance. *Information and Computer Security*, *28*(5), 743–761. https://doi.org/10.1108/ICS-08-2019-0095
Williams, P. (2001). Information Security Governance. In *Information Security Technical Report* (Vol. 6, Issue 3, pp. 60–70). Elsevier Advanced Technology. https://doi.org/10.1016/S1363-4127(01)00309-0
Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets 2013 23:4*, *23*(4), 341–354. https://doi.org/10.1007/S12525-013-0137-3
Wilson, J. M., Lee, J., Fitzgerald, H. N., Oosterhoff, B., Sevi, B., & Shook, N. J. (2020). Job insecurity and financial concern during the COVID-19 pandemic are associated with worse mental health. *Journal of Occupational and Environmental Medicine*, *62*(9), 686–691. https://doi.org/10.1097/JOM.0000000000001962
Wu, D., & Zheng, J. (2021). Social media overload, gender differences and knowledge withholding. *Kybernetes*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/K-06-2021-0482/FULL/XML
Xu, F., Luo, X., & Hsu, C. (2017). Anger or Fear? Effects of Discrete Emotions on Deviant Security Behavior Research in Progress. *Proceedings of the 50th Hawaii International Conference on System Sciences*. http://hdl.handle.net/10125/41644
Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal*, *30*(5), 791–844. https://doi.org/10.1111/ISJ.12271

Yegidis, B. L., & Weinbach, R. W. (1991). *Research Methods for Social Workers*.
Youn, S. Y., Lee, J. E., & Ha-Brookshire, J. (2021). Fashion Consumers' Channel Switching Behavior During the COVID-19: Protection Motivation Theory in the Extended Planned Behavior Framework: *Https://Doi.Org/10.1177/0887302X20986521*, *39*(2), 139–156. https://doi.org/10.1177/0887302X20986521
Zack, E. S., Kennedy, J. M., & Long, J. S. (2019). Can Nonprobability Samples be Used for Social Science Research? A cautionary tale. *Survey Research Methods*, *13*(2), 215–227. https://doi.org/10.18148/SRM/2019.V13I2.7262
Zadig, S. M., & Tejay, G. (2010). Securing IS assets through hacker deterrence: A case study. *General Members Meeting and ECrime Researchers Summit, ECrime 2010*. https://doi.org/10.1109/ECRIME.2010.5706700
Zaščerinska, J., Andreeva, N., Zaščerinskis, M., & Aļeksejeva, L. (2016). ENGLISH FOR ACADEMIC PURPOSES FOR THE CONSTRUCTION OF STUDENTS'SCIENTIFIC IDENTITY. *International Journal for 21st Century Education*, *3*(Special), 121-130.
Zhang, S., Zhao, L., Lu, Y., & Yang, J. (2016). Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social network services. *Information & Management*, *53*(7), 904–914. https://doi.org/10.1016/J.IM.2016.03.006

Appendix A: Cover letter

Dear Prospective Participant,

My name is Popyeni Kautondokwa; I am an MCom Information Systems student at the University of Cape Town conducting a study with the aim of understanding the influence of COVID-19 pandemic-induced contextual factors on employees' information security policy compliance behaviour in organisations in South Africa.

This study has been approved by the UCT Ethics Review Committee of the Faculty of Commerce.
Your participation in this study is voluntary. You can withdraw from the questionnaire at any time.
The questionnaire will take approximately 10-15 minutes to complete.
Participants will not be requested to supply any identifiable information, ensuring anonymity of your responses. All responses will be treated with the utmost confidentiality

Should you have any questions regarding the study, do not hesitate to contact the researcher at ktnpop001@myuct.ac.za.

Regards,

Researcher - Popyeni Kautondokwa
E-mail – ktnpop001@myuct.ac.za

Appendix B: Ethics approval application form

UNIVERSITY OF CAPE TOWN

FACULTY OF COMMERCE

Igniting Knowledge and Opportunity

Commerce Faculty Ethics in Research Application Form

Any person planning to undertake research in the Faculty of Commerce at the University of Cape Town is required to obtain ethical clearance. This form is intended for undergraduate students, honours students, PD Dip students and Masters students whose research component is less than 90 credits.

Once this form is completed it should be sent via email to your departmental ethics representative. Your supervisor will be able to provide you with the contact details.

It is assumed that the researcher has read the UCT Code for Research involving Human Subjects (Available at http://web.uct.ac.za/depts/educate/download/uctcodeforresearchinvolvinghumansubjects.pdf) in order to be able to answer the questions in this form. Students must include a copy of the completed form with the dissertation/thesis when it is submitted for examination.

1. PROJECT DETAILS		
Project title: The influence of COVID-19 contextual factors on information security policy compliance.		
Principal Researcher/s: Popyeni Kautondokwa	**Email address(es):**	ktnpop001@myuct.ac.za
Research Supervisor: Zainab Ruhwanya	**Email address(es):**	zainab.ruhwanya.uct.ac.za
Co-researcher(s): Prof. Irwin Brown	**Email address(es):**	irwin.brown.uct.ac.za
Department: Information Systems		
Brief description of the project: The research project studies the impact that COVID-19 contextual factors have had on the information security compliance of employees in organisations in South Africa.		
Data collection: (please select) ☐Interviews ☑Questionnaire ☐Experiment ☐Secondary data ☐Observation ☐ Other (please specify): _____		
Have you attached a research proposal OR a literature review with research methodology? (please select) ☑Yes ☐No		

2. PARTICIPANTS

2.1 Does the research discriminate against participation by individuals, or differentiate between participants, on the grounds of gender, race or ethnic group, age range, religion, income, handicap, illness or any similar classification?	YES	NO ✕
2.2 Does the research require the participation of socially or physically vulnerable people (children, aged, disabled, etc.) or legally restricted groups?	YES	NO ✕
2.3 Will you be able to secure the informed consent of all participants in the research? (In the case of children, will you be able to obtain the consent of their guardians or parents?)	YES ✕	NO
2.4 Will any confidential data be collected or will identifiable records of individuals be kept?	YES ✕	NO
2.5 In reporting on this research is there any possibility that you will not be able to keep the identities of the individuals involved anonymous?	YES	NO ✕
2.6 Are there any foreseeable risks of physical, psychological or social harm to participants that might occur in the course of the research?	YES	NO ✕
2.7 Does the research include making payments or giving gifts to any participants?	YES	NO ✕

If you have answered **YES to any of these questions**, please describe how you plan to address these issues (append to form):

Affiliations of participants: (please select)

☑Company employees ☐Hospital employees ☐General public ☐Military staff ☐Farm workers ☐Students

☐ Other (please specify): _____

Race / Ethnicity:

Are you asking a question about race/ethnicity in your questionnaire?

☐ Yes ☑No

Which race categories have been used?

Have you included the option: "Prefer not to answer" as part of your race/ethnicity question?

3. PROVISION OF SERVICES

Does your research involve the participation of or provision of services to communities?
If your answer is YES, please complete below:

3.1 Is the community expected to make decisions for, during or based on the research?	YES	NO ✕
3.2 At the end of the research will any economic or social process be terminated or left unsupported, or equipment or facilities used in the research be recovered from the participants or community?	YES	NO ✕
3.3 Will any service be provided at a level below the generally accepted standards?	YES	NO ✕

If you answered YES to any of these questions, please describe below how you plan to address these issues.

3. ORGANISATIONAL PERMISSION

If your research is being conducted within a specific organisation, please state how organisational permission has been/will be obtained:

Have you attached the letter from the organisation granting permission? (please select)

☐ Yes ☐ No, but this **will be** obtained before commencing the research ☑ Not applicable

Are you making use of **UCT students** as respondents for your research? (please select) ☐ Yes ☑ No

If yes, have you contacted Executive Director: Student Affairs for permission? (please select) ☐ Yes ☐ No

Was approval granted? (please select) ☐ Yes ☐ No ☐ Awaiting a response

Are you making use of **UCT staff** as respondents for your research? (please select) ☑ Yes ☐ No

If yes, have you contacted Executive Director: Human Resources for permission? (please select) ☑ Yes ☐ No

Was approval granted? (please select) ☐ Yes ☐ No ☑ Awaiting a response

Contact Emails: Executive Director: Human Resources (Miriam.Hoosain@uct.ac.za)
Executive Director: Student Affairs (Moonira.Khan@uct.ac.za)

4. INFORMED CONSENT

What type of consent will be obtained from study participants?

- ☐ Oral Consent
- ☐ Written Consent
- ☒ Anonymous survey questionnaire (covering letter required , no consent forms needed)
- ☐ Other (Please Specify)

How and where will consent/permission be recorded?

Have you attached an informed consent form to your application? ☑ Yes ☐ No

5. SPONSORSHIP OF RESEARCH

If your research is sponsored, is there any potential for conflicts of interest?
If your answer is YES, please complete below

4.1 Is there any existing or potential conflict of interest between a research sponsor, academic supervisor, other researchers or participants?	YES	NO ✕
4.2 Will information that reveals the identity of participants be supplied to a research sponsor, other than with the permission of the individuals?	YES	NO ✕
4.3 Does the proposed research potentially conflict with the research of any other individual or group within the University?	YES	NO ✕

If you have answered **YES** to any of these questions, please describe how you plan to address these issues (append to form)

6. RISK TO PARTICIPANTS
Does the proposed research pose any physical, psychological, social, legal, economic, or other risks to study participants you can foresee, both immediate and long range? (please select) ☐ Yes ☑No **If yes, answer the following questions:** 1. Describe in detail the nature and extent of the risk and provide the rationale for the necessity of such risks 2. Outline any alternative approaches that were or will be considered and why alternatives may not be feasible in the study 3. Outline whether and why you feel that the value of information to be gained outweighs the risks
1.
2.
3.

I certify that I have read the Commerce Faculty Ethics in Research policy (http://www.commerce.uct.ac.za/Pages/ComFac-Downloads)	☑

I hereby undertake to carry out my research in such a way that

- there is no apparent legal objection to the nature or the method of research; and
- the research will not compromise staff or students or the other responsibilities of the University;
- the stated objective will be achieved, and the findings will have a high degree of validity;
- limitations and alternative interpretations will be considered;
- the findings could be subject to peer review and publicly available; and
- I will comply with the conventions of copyright and avoid any practice that would constitute plagiarism.

Signed by:

	Full name and signature	Date
Principal Researcher/Student: 	Popyeni Kautondokwa	10 November 2021

This application is approved by:

Supervisor		
Departmental Ethics Rep		

Questionnaire checklist on next page

CHECKLIST	SELECT
A full copy of a research proposal or a literature review with methodology is attached in a separate file	☑
Interview schedules / cover letters / questionnaires / forms and other materials used in the study are attached in separate files	☑
Organisational consent letter / UCT student or staff approval letter	☑
On your cover letter to your questionnaire have you included the following?	NA ☑
1. The following UCT Logo 	☑
2. A sentence explaining the aim of the research	☑
3. Sentences of a similar nature to below must be included in the cover letter or consent form:	
This research has been approved by the Commerce Faculty Ethics in Research Committee.	☑
Your participation in this research is voluntary. You can choose to withdraw from the research at any time.	☑
The questionnaire will take approximately X minutes to complete	☑
You will not be requested to supply any identifiable information, ensuring anonymity of your responses.	☑
Due to the nature of the study you will need to provide the researchers with some form of identifiable information however, all responses will be confidential and used for the purposes of this research only.	OR ☑
Should you have any questions regarding the research please feel free to contact the researcher (insert contact details).	☑
4. Have you scanned in your signature for the last section of the form?	☑

Ethics Approval Request for the Study entitled:

Signed by:

	Full name and signature	Date
Principal Researcher/Student: Popyeni Kautondokwa	Popyeni Kautondokwa	15 November 2020

This application is approved by:

Supervisor		
Co- Supervisor		

Appendix C: Ethics clearance

Faculty of Commerce

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

24 11 2021

Popyeni Kautondokwa

Department of Information Systems

University of Cape Town

REF: REC 2021/11/020

The influence of COVID-19 contextual factors on information security policy compliance.

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 31-Dec-2022 .

Your clearance may be renewed upon application.

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

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

We wish you well for your research.

2021.11.24
14:12:02 +02'00'

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

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

Appendix D: Outer loadings

	COM	FR	IO	JI	ME1	ME2	ME3	PA	PR	TC	TCI	TS
AF1		0.882										
AF2		0.914										
AF3		0.886										
AF4		0.896										
AF5		0.916										
AF6		0.925										
AF7		0.878										
COMP1	0.941											
COMP2	0.928											
COMP3	0.929											
COMP4	0.902											
IO * TCI							1.033					
IO1			0.842									
IO2			0.928									
IO3			0.888									
IO4			0.858									
JI * FR					0.947							
JI1				0.899								
JI2				0.893								
JI3				0.952								
PA1								0.863				
PA2								0.900				
PA3								0.941				
PA4								0.928				
PA5								0.908				
PR1									0.854			
PR2									0.853			
PR3									0.899			
PR4									0.887			
TELE1										0.874		
TELE2										0.836		
TELE3										0.899		
TELE4										0.897		
TI1											0.961	

	COM	FR	IO	JI	ME1	ME2	ME3	PA	PR	TC	TCI	TS
TI2											0.958	
TI3											0.959	
TI4											0.961	
TI5											0.910	
TI6											0.940	
TS * TCI						1.028						
TS2												0.853
TS3												0.859
TS5												0.861

Appendix E: Gender Step 3 MICOM

MOD: Mean Original Difference
MP: Mean Permutation
MD: Mean Difference
VOD: Variance Original Difference
VPMD: Variance Permutation Mean Difference

	MOD (Female - Male)	MP MD (Female - Male)	5%	95%	Permutation p-Values	VOD (Female - Male)	VPMD (Female - Male)	5%	95%	Permutation p-Values
COM	0.168	0.000	-0.170	0.174	0.110	-0.064	0.008	-0.420	0.384	0.827
FR	0.462	0.008	-0.202	0.188		-0.674	0.005	-0.313	0.354	0.003
IO	0.209	0.004	-0.178	0.194	0.067	-0.233	0.012	-0.218	0.222	0.087
JI	0.019	0.001	-0.182	0.209	0.867	0.104	0.005	-0.192	0.200	0.387
ME1	-0.148	0.008	-0.158	0.190	0.187	-0.620	0.003	-0.409	0.422	0.017
ME2	-0.043	-0.007	-0.212	0.169	0.713	0.218	0.011	-0.272	0.283	0.230
ME3	0.047	0.003	-0.199	0.208	0.737	-0.100	0.010	-0.282	0.277	0.533
PA	0.090	0.001	-0.217	0.186	0.443	-0.168	0.016	-0.551	0.545	0.587
PR	0.085	-0.002	-0.196	0.173	0.453	-0.137	0.010	-0.406	0.448	0.620
TC	0.104	-0.011	-0.190	0.167	0.383	-0.170	0.021	-0.252	0.322	0.343
TCI	-0.081	-0.003	-0.208	0.191	0.517	0.230	0.002	-0.114	0.130	
TS	-0.004	-0.003	-0.208	0.184	0.987	0.055	0.009	-0.212	0.209	0.680