UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Empirical investigation of the determinants of cybersecurity behaviour among South Africans

by

Sindisiwe Sampson
14006040

Submitted in fulfilment of the requirements for the degree
MCom Informatics

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at the

UNIVERSITY OF PRETORIA

Supervisor
(Dr Funmi Adebesin)

Date of submission
(31 July 2023)

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Declaration regarding Plagiarism

The Department of Informatics emphasises integrity and ethical behaviour with regard to the preparation of all written assignments.

Although the lecturer will provide you with information regarding reference techniques, as well as ways to avoid plagiarism, you also have a responsibility to fulfil in this regard. Should you at any time feel unsure about the requirements, you must consult the lecturer concerned before submitting an assignment.

You are guilty of plagiarism when you extract information from a book, article, web page or any other information source without acknowledging the source and pretend that it is your own work. This doesn't only apply to cases where you quote verbatim, but also when you present someone else's work in a somewhat amended (paraphrased) format or when you use someone else's arguments or ideas without the necessary acknowledgement. You are also guilty of plagiarism if you copy and paste information directly from an electronic source (eg, a web site, email message, electronic journal article, or CD ROM), even if you acknowledge the source.

You are not allowed to submit another student's previous work as your own. You are furthermore not allowed to let anyone copy or use your work with the intention of presenting it as his/her own.

Students who are guilty of plagiarism will forfeit all credits for the work concerned. In addition, the matter will be referred to the Committee for Discipline (Students) for a ruling. Plagiarism is considered a serious violation of the University's regulations and may lead to your suspension from the University. The University's policy regarding plagiarism is available on the Internet at *http://upetd.up.ac.za/authors/create/plagiarism/students.htm*.

I (full names & surname):	Sindisiwe Anawi Sampson
Student number:	14006040

Declare the following:

1. I understand what plagiarism entails and am aware of the University's policy in this regard.
2. I declare that this assignment is my own, original work. Where someone else's work was used (whether from a printed source, the Internet or any other source) due acknowledgement was given and reference was made according to departmental requirements.
3. I did not copy and paste any information directly from an electronic source (eg, a web page, electronic journal article or CD ROM) into this document.
4. I did not make use of another student's previous work and submitted it as my own.
5. I did not allow and will not allow anyone to copy my work with the intention of presenting it as his / her own work.

Signature

Date

Table of Contents

Appendices

List of Figures

List of Tables

Empirical investigation of the determinants of cybersecurity behaviour among South Africans

Abstract

Cybercrime is a borderless threat that affects both developed and developing countries and continues to grow. According to the International Business Machines Corporation (IBM), in 2022 the average cost of data breach across the globe was $4.35 million. The COVID-19 pandemic significantly accelerated the digital landscapes of many countries, including South Africa. Subsequently, there was an increase in incidents of cyberattacks globally.

Good cybersecurity behaviour encompasses the actions undertaken by individuals to protect their data, devices, and networks from cyberattacks. Consequently, this study investigated the factors that could influence the cybersecurity behaviours of South Africans and determine the factors that could exert the greatest impact on their cybersecurity behaviours.

The study employed an online questionnaire to collect data from a sample of 329 South African participants. The theoretical frameworks used included Theory of Planned Behaviour (TPB) and the Protection Motivation Theory (PMT).

The findings revealed that an individual's intention to engage in good cybersecurity behaviours is significantly influenced by their Attitude towards good cybersecurity behaviours, Subjective norms, Perceived severity, and Response efficacy. Moreover, the study results revealed Perceived severity as a mediator in the relationship between Perceived vulnerability and Intention to practice good cybersecurity behaviours. The research findings underscore the importance of influencing these factors to effectively promote good cybersecurity behaviours amongst South Africans. Targeting and changing Attitudes towards good cybersecurity behaviours, Subjective norms, Perceived severity, and Response efficacy, could increase the practice of good cybersecurity behaviours in South Africans and mitigate the risks associated with cyberthreats.

Keywords: Cybersecurity, Cybersecurity behaviour, South Africa, Information security behaviour, Theory of Planned Behaviour, Protection Motivation Theory.

Chapter 1 Introduction

The World Economic Forum listed widespread cybercrime and cyber insecurity amongst the top ten global risks for the short term (next two years) and long term (next ten years) (World Economic Forum, 2023). Cybercrime continues to be a borderless threat that affects both developed and developing countries while growing in both size and scope (de Bruijn & Janssen, 2017; Peters & Jordan, 2019). Around the world, there is an increase in the number of cyber incidents occurring, but there has also been a significant increase in cyber incidents on the African continent (Kshetri, 2019). As the volume of cyber incidents increases, so too does the cost associated with these incidents. The International Business Machines Corporation (IBM) reports the average global cost of a data breach in 2022 to be an estimated $4.35 million (IBM Security, 2022). Around the world, countries are struggling to mitigate the impact of cybercrime on citizens, governments and organisations (Peters & Jordan, 2019).

South Africa is no stranger to the cyberworld and technology, with immense growth in the number of Internet users in the country (Kemp, 2023). Due to the Coronavirus pandemic which started in 2019 (COVID-19), there was a shift in how people socialise and conduct business (Naidoo, 2020). Many people had to convert to working and socialising from home using the Internet. Unsurprisingly, cybercriminals exploited the COVID-19 pandemic and as a result, end-user cyberattacks were on the rise worldwide (Mtuze & Musoni, 2023; Naidoo, 2020). Cyberattacks evolved to fit the context of COVID-19 by focusing on remote workers and curated COVID-19-related scams on end-users (Naidoo, 2020). One of the significant cybersecurity concerns in Africa is that Internet users lack experience with technology and are not as technically inclined as the more developed countries, which means that users may not know how to protect and defend themselves against cyberattacks (Kshetri, 2019).

The growth of cyber incidents across the African continent can be accredited to the vulnerability of systems and the laid-back approach to good cybersecurity practices (Kshetri, 2019). Cybersecurity continues to go un-emphasised in South Africa (Pieterse, 2021), which could be attributed to the fact that cybersecurity is considered a luxury in most African economies (Kshetri, 2019). However, given that cyberattacks are growing increasingly dangerous to individuals, organisations, and the country's digital infrastructure, cybersecurity in South Africa should be considered as a necessity (Mitrovic, Colab, Thakur & Phukubje, 2019). Laws, regulations and policies governing cyber incidents continue to lag, while the cyberspace continues to grow (Dill, 2018; Pieterse, 2021).

In 2020, one of South Africa's prominent banks, Nedbank, experienced a significant data breach incident, where 1.7 million clients' data records were compromised due to the fault of a third-party marketing organisation (Nedbank, 2020). IBM estimates that in South Africa, the average organisational cost of a data breach is around $3.36 million (IBM Security, 2022), which may seem insignificant to a huge corporation, but it can be detrimental to smaller organisations. In South Africa, there is little emphasis on the awareness, implementation, and regulation of cybersecurity. If left unaddressed, this phenomenon could start to have a much more significant impact on businesses and individuals in the country (Mitrovic et al., 2019).

Many studies have warned that humans are the weakest link regarding cybersecurity (Bulgurcu, Cavusoglu & Benbasat, 2010; Donalds & Osei-Bryson, 2020; Pham, Brennan & Richardson, 2017; Yoon & Kim, 2013; Zwilling, Klien, Lesjak, Wiechetek, Cetin & Basim, 2020). The most common cause of security issues are users who do not follow proper security procedures and behaviours (Pham et al., 2017; Yoon & Kim, 2013). Understanding the factors that influence users' engagement in good cybersecurity behaviours is vital in contemporary times. This comprehension has the potential to enhance overall cybersecurity postures and effectively mitigate the consequences of cyberattacks (Almansoori, Al-Emran & Shaalan, 2023; Moustafa, Bello & Maurushat, 2021). This study sought to determine the factors that could influence the practice of good cybersecurity behaviours by South African citizens while online. This study aimed to understand what factors might have the most significant impact on good cybersecurity behaviour by South African Internet users.

1.1 Problem statement

Cybersecurity awareness is an important yet complex challenge facing South Africa (Gcaza & von Solms, 2017; Mitrovic et al., 2019; Pieterse, 2021; Veerasamy, Mashiane & Pillay, 2019). Cyberattacks, such as violation of privacy, identity theft and credit card fraud (Thomas, 2018; Zwilling et al., 2020), unauthorised system compromises (Veerasamy et al., 2019) or curated scam / phishing emails (Naidoo, 2020) can have adverse effects on the lives of South Africans and their businesses. The impact of not practising good cybersecurity behaviours can be severe and so it becomes vital to understand the behaviours and processes individuals follow and to investigate the determinants of these behaviours (Bulgurcu et al., 2010; Crossler & Bélanger, 2014).

This study aimed to evaluate and understand the factors that might influence South Africans to practise good cybersecurity behaviours. In South Africa, current research on this topic focuses on developing different strategies to increase public cybersecurity awareness by creating a good cybersecurity culture (de Bruijn & Janssen, 2017; Gcaza & von Solms, 2017) or addressing the cybersecurity skilling issue (Mitrovic et al., 2019). Other studies focus on evaluating awareness and implementing awareness initiatives in local or rural communities (Grobler, Dlamini, Ngobeni & Labuschagne, 2011; Grobler, Jansen van Vuuren & Zaaiman, 2013) or the education system (Kritzinger, Bada & Nurse, 2017) in South Africa. Some studies focus on existing and proposed strategies for developing and implementing effective cybersecurity policies and frameworks in South Africa (Grobler, Jansen van Vuuren & Leenen, 2012; Mtuze & Musoni, 2023; Sutherland, 2017).

Many international studies researched the factors influencing good cybersecurity behaviours, but the results are varied and range from country to country (Crossler & Bélanger, 2014; Yoon & Kim, 2013). There seems to be a deficiency of research into the wide range of factors that might influence and impact South Africans practising good cybersecurity behaviours. Most of the research conducted in South Africa focuses on awareness and implementation of awareness in the country, but this does not give enough context as to whether awareness is the issue or if other factors might be playing a part in South Africans' good cybersecurity behaviour. There is little to no research into what might influence a South African citizen to practice good cybersecurity behaviour.

Therefore, this study investigated the factors that might influence South African citizens to practice good cybersecurity behaviour to protect themselves while online. The potential impact of not addressing the cybersecurity issue in South Africa could be detrimental, not only to individuals but also to the national infrastructure (Grobler et al., 2013; Mitrovic et al., 2019).

1.2 Justification

Globally, cyber incidents are growing, and cybersecurity is becoming more vital. South Africa is quickly becoming more reliant on information and communication technology (ICT) to provide essential services (van Vuuren, Grobler, Leenen & Phahlamohlaka, 2014), therefore the country should ensure that they understand the increased cybersecurity risks that they may face (van Vuuren et al., 2014; Veerasamy et al., 2019). Different cyber incidents can range in threat level from a harmless spam threat to a much more catastrophic threat (Zwilling et al., 2020) like nation-wide data breaches. Data breaches are a more extreme issue in South Africa, as they occur more often than other cyber incidents (Pieterse, 2021; Van Niekerk, 2017; Veerasamy et al., 2019). Data breaches can impact all the stakeholders in our society (de Bruijn & Janssen, 2017); they are not limited to individuals or organisations. Cybersecurity awareness and training programmes are used to share knowledge on cybersecurity risks and encourage practising good cybersecurity behaviour (Gundu, 2019; Kritzinger et al., 2017). Researchers have found that an individual's good cybersecurity behaviours play a vital part in preventing cyberattacks (Almansoori et al., 2023; Moustafa et al., 2021).

1.3 Research question and objectives

The main research question for this study is: *What are the factors that could influence South Africans to practise good cybersecurity behaviours?* The following research sub-questions support the main research question:

- Which of the identified factors has the most significant impact on South Africans' intention to practise good cybersecurity behaviours?
- What is the influence of an individual's education level and time spent on the Internet daily on the intention to practise good cybersecurity behaviours?

1.4 Significance of the study's contribution

Understanding the factors that influence users' engagement in good cybersecurity behaviours is vital in contemporary times. This comprehension has the potential to enhance overall cybersecurity postures and effectively mitigate the consequences of cyberattacks (Almansoori et al., 2023; Moustafa et al., 2021). Therefore, the audiences that will benefit from this study include South African citizens, academics, policymakers, the Government, regulators, and organisations in South Africa. Academics, regulators, organisations, and the Government will benefit from this study by gaining more insight into the factors that influence South Africans to practise good cybersecurity behaviours, which can be used in their future cybersecurity awareness strategies. This information could also potentially be utilised in the future as the basis for other researchers' studies.

1.5 Delineation and limitation

The data for this study was collected from individuals who are residents in South Africa, who voluntarily participated in the survey. Hence, the results may not be generalisable to the entire population.

1.6 Brief chapter overview

The dissertation consists of five chapters:

Chapter one provides an introduction to this study as well as the problem statement, justification, research questions and objectives, significance of the study's contribution and limitations.

Chapter two provides a review of available literature on the current cyberthreat landscape in South Africa and a review of international studies focusing on good cybersecurity behaviours and the determinants of those behaviours.

Chapter three presents the methodology used in this study. This includes a discussion of the theoretical framework used, the research strategy, sampling, data collection procedure and the research instrument.

Chapter four provides an analysis of the findings from the data collected in this study. This includes the statistical methodologies used to analyse the data collected.

Chapter five presents a general discussion of results and the conclusion of this study. This includes the summary of findings, implications for theory and practise and the conclusion.

Chapter 2 Literature review

2.1 Introduction

This chapter contextualises the phenomenon of good cybersecurity behaviour discussed in this study, extant literature on cybersecurity and the cyberthreat landscape in South Africa is discussed in section 2.2. Section 2.3 discusses some of the available, mostly international, research into the possible determinants of an individual’s good cybersecurity behaviour.

2.2 The cyberthreat landscape in Africa and South Africa

Around the world, there has been an increase in the number of cyber incidents occurring, but there has also been a significant increase in cyber incidents on the African continent (Kshetri, 2019; Mphatheni & Maluleke, 2022). The cyberthreat landscape in Africa has evolved significantly, reflecting both the technological advancements and vulnerabilities of the continent (Mphatheni & Maluleke, 2022). Despite the fact that Africa's digital transformation has produced significant socioeconomic gains, it has also made the continent vulnerable to a wide range of cyber risks (Peter, 2017). Various factors contribute to the complex and growing cyberthreat landscape in Africa, including weak cybersecurity infrastructure, insufficient legislative frameworks, and the rapid adoption of digital technologies without effective security measures (Ifeanyi-Ajufo, 2023; Kshetri, 2019; Mphatheni & Maluleke, 2022). Furthermore, the proliferation of mobile devices and the rising rates of Internet usage have significantly expanded the attack surface, increasing the vulnerability of individuals and organisations. (Interpol, 2023).

A report published by Interpol in 2023, called the African Cyberthreat Assessment Report lists the most prominent cyberthreats identified in the African region (Interpol, 2023). These cyberthreats include phishing, ransomware attacks, business email compromise, banking trojans and stealers, online scams and cyber extortions (Interpol, 2023). The countries in Africa differ significantly in terms of their capacities, competencies and financial resources (Ifeanyi-Ajufo, 2023; Interpol, 2023). While some African countries have highly qualified and skilled professionals with investigative capabilities and equipment, others are only recently beginning to develop and implement fundamental legal and regulatory frameworks to combat cybercrime (Ifeanyi-Ajufo, 2023; Interpol, 2023). Moreover, the vulnerability of African nations to cyberthreats is exacerbated by underdeveloped systems infrastructure and the lack of access to basic infrastructure needed to enable maximum efficiency of digital technologies and cyber protection measures like electricity (Ifeanyi-Ajufo, 2023). One of the significant cybersecurity concerns in Africa is that Internet users lack experience with technology and are not as technically inclined as the more developed countries, which means that users may not know how to protect and defend themselves against cyberattacks (Kshetri, 2019). However, despite the multitudes of complex issues facing the African nations, cybersecurity legislation, cybercrime strategies and protection measures in Africa are gradually improving, especially in the private sector (Interpol, 2023; Kshetri, 2019; Peter, 2017).

South Africa has a total population of 60.14 million people, and 43.48 million of those people are Internet users (Kemp, 2023). That means South Africa has a 72.3% Internet penetration rate (Kemp, 2023). The continued growth of Internet users and Internet-capable devices means that there is an increase in attack vectors, which are ways to carry out cybercrime (Mtuze & Musoni, 2023; Peters & Jordan, 2019). It was reported that 77.5% of households in South Africa have at least one member who has access to the Internet (Statistics South Africa, 2021). At 89.1% of households, the Western Cape has the highest access to the Internet (Statistics South Africa, 2021).

The South African National Cybersecurity Hub (hereafter ‘the Hub’), under the Department of Telecommunications and Postal Services, is mandated to oversee the coordination of activities related to information dissemination, the creation of awareness and the development of standards on cybersecurity (Cybersecurity Hub, 2019). Some of the services provided by the Hub to citizens and organisations include (Cybersecurity Hub, 2019):

- Alerts and warnings of cyber incidents.
- Awareness building.
- Incident handling.
- Incident response support.
- Cybersecurity-related information sharing.

The Hub plays a vital role in upholding the National Cybersecurity Policy Framework (NCPF), which was passed in 2012 to help South Africa adequately address the issue of cybersecurity (Cybersecurity Hub, 2019). Though conducting national surveys on cybersecurity readiness is a mandate of the Hub, only one national survey on cybersecurity readiness has been conducted since its inception (Cybersecurity Hub, 2019). The Hub does not share reported incidents with the general public (Pieterse, 2021). In 2018, it was reported in the media that a member of the Hub admitted that the Hub is incredibly under-resourced (Mitrovic, 2018).

Due to a lack of published information on cybersecurity statistics in South Africa, researchers turn to industry and academia for information. Industry-led research reports and private company reports are the main sources used to highlight cybersecurity and cybercrime statistics in South Africa (Pieterse, 2021).

In a report released by a private cybersecurity company called Surfshark (Surfshark, 2022), South Africa ranked fifth on a global ranking list of cybercrimes in 2022, . In a PricewaterhouseCoopers (PwC) 2020 economic crime survey, cybercrime was listed in the top five of economic crime / fraud experienced in South Africa (PricewaterhouseCoopers, 2020). During their annual ‘Cybersecurity Weekend’, Kaspersky Lab revealed that they found Android smartphones in South Africa are the second-most targeted devices using banking malware (Shapshak, 2019). Kaspersky Lab’s findings can be supported by South Africa’s Banking Risk Information Centre (SABRIC), which reported that from 2020 to 2021, there was an increase in gross losses attributable to digital banking fraud, from approximately R310 million to R438 million (South African Banking Risk Information Centre, 2021).

There are very few peer-reviewed articles published that evaluate and investigate cyber incidents in South Africa (Pieterse, 2021). One study by Van Niekerk (2017) evaluated and classified 54 cyber incidents that took place in South Africa between 1994 and 2016. According to Van Niekerk (2017), data exposure and financial theft were the topmost cyberattack impacts that occurred. However, this study was limited to information that was publicly reported, since at the time it was conducted it was not a mandatory requirement to report cyber incidents in South Africa (Van Niekerk, 2017). A more recent study was published by Pieterse (2021) that analysed 74 newsworthy cyber incidents in South Africa between 2010 and 2020. Pieterse (2021) noted an increase in cyber incidents over the past decade, with the majority of cyber incidents in South Africa occurring in 2019 (19 cyber incidents). The findings were similar to van Niekerk (2017) in that the most prevalent cyber incident type was data exposure, followed by compromised websites (Pieterse, 2021). Pieterse (2021) also found that hackers were the most common perpetrator type, with more than half of the cyber incidents analysed being perpetrated by hackers. These findings by Pieterse (2021) indicate just how attractive South Africa is to cybercriminals. The study also noted key elements that are negatively affecting South Africa's cyberthreat landscape, based on a report by the private company Accenture. The elements include lack of investment in cybersecurity, slow development of cybercrime legislation, lack of awareness of cyberthreats, and increasing use of IT (Pieterse, 2021).

Gcaza & von Solms (2017) investigated the environmental factors that contribute to the absence of a cybersecurity-focused culture in South Africa. The authors found that these factors include a "lack of government-led awareness / research initiatives" (Gcaza & von Solms, 2017). "Lack of accountability" from the Government was also mentioned, as efforts to cultivate a cybersecurity culture in South Africa are mainly championed by academia, industry, and international groups (Gcaza & von Solms, 2017).

In the year 2020, during the COVID-19 pandemic, South Africa faced two big privacy-related issues, which made the citizens more aware of what their data is being used for than ever before. The first issue was the South Africa 'COVID Alert SA' mobile application, and the second issue were the changes to the WhatsApp privacy policy. Both issues will be discussed to add context to the issue of cybersecurity awareness in South Africa.

COVID-19 contributed significantly to the change in the global and South African cybersecurity landscape with a huge migration to working remotely and e-learning by companies and institutions (Carugati, Mola, Plé, Lauwers & Giangreco, 2020; Jere, 2020; Naidoo, 2020). Due to COVID-19, there was an exponential increase in the adoption of e-learning in higher education institutions worldwide (Jere, 2020). Almost all of the universities in South Africa have implemented some form of e-learning (Jere, 2020). Organisations had to quite quickly make the transition to employees working remotely, and this created more potential security threats (Williams, Chaturvedi & Chakravarthy, 2020). Employees at home could potentially be using outdated and unsecure devices or networks more than they would at work (Naidoo, 2020; Williams et al., 2020). The transition to digital platforms of both students and working adults resulted in a rise in online users. Concurrently, the global pandemic further fuelled this increase. Consequently, it is expected that the prevalence of cyberattacks will also escalate. Globally, when a phenomenon like a pandemic or natural disaster occurs, cybercriminals take advantage of this to create more curated, authentic-looking scams and websites often imitating trusted organisations like the World Health Organization (WHO) (Naidoo, 2020; Williams et al., 2020). COVID-19 contributed to an increase in COVID-19 curated end-user cyberattacks worldwide (Naidoo, 2020; Wirth, 2020).

During the COVID-19 pandemic there was a need for increased availability and use of technology to develop and enable COVID-19 tracking and tracing via smartphone applications globally (Dwivedi, Hughes, Coombs, Constantiou, Duan, Edwards, Gupta, Lal, Misra, Prashant, Raman, Rana, Sharma & Upadhyay, 2020) and in South Africa. However, in South Africa there were real concerns about privacy and tracking individuals' movements through the 'COVID Alert SA' application (Bhana, 2020). The concern stemmed from South Africa's 'Tracing Database', established in April 2020 (Klaaren, Breckenridge, Cachalia, Fonn & Veller, 2020). This database contained personal and identifiable data, mobility and locational data on those tested for COVID-19, and their listed contacts (Klaaren et al., 2020). The mobility data was collected from mobile phone operators who were required to share the location and movements of those individuals suspected of or had confirmed contracting COVID-19 (Bhana, 2020; Klaaren et al., 2020). This database infringed on an individual's constitutional right to privacy (Botes, 2020). In order to gain public trust, it was announced that the 'COVID Alert SA' application did not store or record an individual's personal information or their geo-location, but rather generated a random code which was linked to a person's mobile device (Bhana, 2020; Botes, 2020).

Also in 2020, Facebook issued a notice to WhatsApp users, asking them to accept an update to their privacy policy and terms of service. This update caused a huge uproar in the South African community and resulted in many negative media reports

(BusinessTech, 2021; MyBroadband, 2021). Many WhatsApp users then migrated to other messaging apps like Telegram and Signal in response to WhatsApp's update (MyBroadband, 2021). The updates to the policies included how WhatsApp and Facebook share data between the applications and how WhatsApp processes users' data (BusinessTech, 2021). WhatsApp does not collect 'chats', as those are encrypted, but it does collect phone numbers of users and their contacts, profile pictures, profile names and other diagnostic data (BusinessTech, 2021). The local uproar was so negative that the South African Government institutions had to step in and address the issue. On 13 January 2021, the Information Regulator of South Africa stated that they would be investigating the changes to the WhatsApp privacy policy to ensure that changes align to South Africa's privacy laws (Information Regulator South Africa, 2021). This issue heightened the awareness of South African citizens about the extent to which their personal data is being used without their knowledge.

The Protection of Personal Information (POPI) Act came into effect in South Africa on 1 July 2020 and is regulated by the Information Regulator of South Africa (Government Gazette, 2013). The primary objective of the POPI Act is to control how private and public bodies handle personal information, ensuring that people's right to privacy is protected (Government Gazette (2013). The purpose of the POPI Act is to set guidelines, methods and standards for the ethical and responsible gathering, use, storage and disclosure of personal data (Government Gazette, 2013). It establishes requirements for corporations to manage personal information securely and openly, and gives individuals more control over their personal data (Government Gazette, 2013). According to the Act, businesses must seek authorisation before processing personal information, keep it accurate, and take the necessary precautions to prevent loss, theft, or destruction (Government Gazette, 2013). Additionally, it gives people the ability to access and update any personal information that is held about them. POPI act violations can result in fines and other serious legal repercussions for violations (Government Gazette, 2013). The Act's overall goal is to improve data protection and privacy in South Africa while bringing the nation into line with international best practices for the digital age (Michalsons, 2022).

2.3 Cybersecurity behaviour

Cybersecurity can be defined as the process of protecting information systems and the data they contain from malicious damage, modification, exploitation or unauthorised use or access (Evans, Maglaras, He & Janicke, 2016). Cybersecurity behaviour is referred to by many different names in the different literature that was analysed. It can be referred to as security practices (Crossler & Bélanger, 2014), security policy compliance (Hassandoust, Techatassanasoontorn & Singh, 2020; Ifinedo, 2012; Jalali, Bruckes, Westmattelmann & Schewe, 2020), information security (Johnston & Warkentin, 2010), cyber hygiene (Cain, Edwards & Still, 2018), protective behaviours (Braun, 2014), and computer security-related behaviours (Yoon & Kim, 2013).

However, no matter what it is called, cybersecurity behaviour refers to the actions taken by an individual to protect their data, computing devices and networks from malicious online information technology (IT) threats called cyberattacks (Braun, 2014; Crossler & Bélanger, 2014). These good cybersecurity behaviours include:

- The use of technical protective solutions (antivirus software, firewalls, spam-filters) (Braun, 2014; Cain et al., 2018; Crossler & Bélanger, 2014; Hassandoust et al., 2020).
- Regular data backups (Chen & Zahedi, 2016; Crossler & Bélanger, 2014; Hassandoust et al., 2020).
- Frequently updating the operating system on computing devices (Chen & Zahedi, 2016; Crossler & Bélanger, 2014).
- Strong password use (Cain et al., 2018; Chen & Zahedi, 2016; Crossler & Bélanger, 2014).
- Identifying and adequately responding to phishing emails (Cain et al., 2018).
- Not posting or sharing personal information online (Cain et al., 2018; Jansen & van Schaik, 2019).
- Not using unsecured, public Wi-Fi hotspots (Cain et al., 2018).

Cybersecurity behaviour has previously been researched at three different levels: an individual or user level, a group level, and an organisational level (Hassandoust et al., 2020). This study is focused on cybersecurity behaviour on an individual level in South Africans but will discuss relevant literature related to the practice of good cybersecurity behaviour, regardless of the level analysed in the research.

Researchers use different models and theories to attempt to investigate and explain individual cybersecurity behavioural intentions and the determinants. Measuring an individual's actual cybersecurity behaviour is challenging (Crossler, Johnston, Lowry, Hu, Warkentin & Baskerville, 2013; Pham et al., 2017), and therefore the majority of these studies focus on an individual's reported behavioural intentions; what the individual says they will do, not what they do in reality (Sommestad, Karlzén & Hallberg, 2014b). However, most research posits that behavioural intention has a substantial impact on actual behavioural adoption (de Bruijn & Janssen, 2017; Siponen, Pahnila & Mahmood, 2010; Sommestad, Hallberg, Lundholm & Bengtsson, 2014a; Yoon & Kim, 2013).

Several studies attempted to examine individual cybersecurity behaviour in an organisational context regarding organisation security policy compliance (Bulgurcu et al., 2010; Ifinedo, 2012; Siponen et al., 2010; Vance, Siponen & Pahnila, 2012; Yoon & Kim, 2013).

In Finland, an empirical study by Siponen et al. (2010) used a combination of theories to investigate and explain employee security policy compliance (Siponen et al., 2010). The theories used include the Theory of Reasoned Action, Protection Motivation Theory (PMT), Deterrence Theory, Theory of Innovation Diffusion and Rewards (Siponen et al., 2010). The researchers found that some constructs (Social norms, Threat appraisal, Self-efficacy, Visibility & Deterrence) had a significant effect on an employee's intention to comply with the security policy and actual compliance (Siponen et al., 2010). A significant recommendation of the study is that awareness of security threats, and their severity through training and education is imperative in the battle against cyberattacks (Siponen et al., 2010).

Another empirical study made use of the Theory of Planned Behaviour (TPB) and Risk Compensation Theory to identify factors that influence individual security policy compliance (Zhang, Reithel & Li, 2009). The factors tested in the study included

Subjective norms, Perceived behavioural control, Attitude towards security behaviours and Perceived security protection mechanism (Zhang et al., 2009). It was found that Perceived behavioural control, Attitude and Perceived security protection mechanism have a significant impact on security compliance Behavioural Intention (Zhang et al., 2009).

A study by Vance et al. (2012) investigated the Behavioural Intention of employees using the PMT and habitual behaviour. It was found that habitual security compliance had a significant influence on the constructs of PMT (Vance et al., 2012). This means that an employee's past and current habitual security behaviours influence their Perceived severity, Perceived vulnerability, Response efficacy, Self-efficacy and Response cost, which in turn influences the intention to comply with the organisation's security policy (Vance et al., 2012). However, the authors found that contrary to their hypotheses, vulnerability has a minor effect on Behavioural Intention.

The study by Yoon & Kim (2013) conducted in Korea, used a similar approach to Vance et al. (2012). The study found that Attitude, Moral obligation and Organisational norms have a substantial impact on Behavioural Intentions (Yoon & Kim, 2013). The researchers included organisational context factors (Organisational norms, organisation's security policy). They found that these factors were shown to have a significant impact on employees' security compliance Behavioural Intention (Yoon & Kim, 2013). This finding supports the present-day perspective of companies emphasising performing security behaviours to their employees as part of their duties (Yoon & Kim, 2013).

The study by Sommestad et al. (2014b) analysed the sufficiency of the TPB in explaining compliance of an organisation's information security policy (Sommestad et al., 2014b). The study tested the TPB and the PMT constructs as well as Anticipated regret; they also measured the respondents' reported Perceived behavioural control (Sommestad et al., 2014b). The results from the study found that the TPB can be enhanced by including Anticipated regret or the variables in the threat appraisal process from PMT (Perceived vulnerability and Perceived severity) (Sommestad et al., 2014b). Alternatively, they suggest replacing some of the TPB constructs with other constructs that are more suited to security policy compliance (Sommestad et al., 2014b).

A study by Ifinedo (2012) in Canada, integrated both PMT and TPB to investigate security policy compliance behaviour in an organisation (Ifinedo, 2012). The study found that the factors of Perceived severity and Response cost were not predictors of behavioural compliance intention (Ifinedo, 2012). The most important aspect of the study was that it validated the combined use of PMT and TPB to better understand the factors that might influence cybersecurity behaviour (Ifinedo, 2012).

In an inter-country study conducted by Chen & Zahedi (2016), PMT was used to analyse and compare individuals' cybersecurity behaviour in the United States of America and China (Chen & Zahedi, 2016). The study proposed using a context-specific approach to investigate security behaviours in individuals across different countries (Chen & Zahedi, 2016). The study included new variables in the proposed model, such as Seeking help, Taking protective actions and Avoidance (Chen & Zahedi, 2016). The results of the study showed that there was a significant difference in the perceptions of security threats and coping appraisals across the different countries, which influence the practice of cybersecurity behaviours at an individual and country level (Chen & Zahedi, 2016). The study by Chen & Zahedi (2016) serves as a justification for this study since perceptions of cybersecurity threats and coping appraisals in South Africa might also present differently.

Where other studies chose to analyse a specific cyberthreat and user behaviour, Crossler & Bélanger (2014) propose adopting a more unified approach. The study proposes the use of a Unified Security Practices Instrument when investigating the practice of cybersecurity behaviours in individuals (Crossler & Bélanger, 2014). The instrument focuses on analysing cybersecurity behaviours using a broader and more standardised measure of technical protective solutions and is not focused on one cybersecurity behaviour like the use of antivirus software (Crossler & Bélanger, 2014). The instrument was empirically tested in the study and was validated by the results gathered (Crossler & Bélanger, 2014).

A study by Jalali, Bruckes, Westmattelmann and Schewe (2020) examined the relationship between compliance intention and compliance behaviour by conducting simulated phishing email tests on hospital staff (Jalali et al., 2020). The study was the only study reviewed that observed and compared Behavioural Intention with actual behaviour. The findings indicated that Attitude towards security compliance, Subjective norms and Perceived behavioural control are significant influencers of intention to comply (Jalali et al., 2020). It was also found that Collective trust positively relates to Subjective norms and Attitudes towards security compliance (Jalali et al., 2020). High workload was also found to be significantly positively related to the likelihood of clicking on a phishing email link (Jalali et al., 2020). Jalali et al. (2020) found no significant relationship between intention and actual compliance (Jalali et al., 2020). Though the finding contradicts prior literature that posits that intention translates to actual behaviour, the authors indicate that further investigation is necessary in different contexts (Jalali et al., 2020).

2.4 Conclusion

In summary, this chapter provided an exploration of the intricate nature of the cyberthreat landscape in South Africa. It sought to demonstrate that it is continuously expanding alongside the evolution of the digital landscape. Existing research on South African cybersecurity concerns focused predominantly on the lack of awareness and absence of a cybersecurity-oriented culture, along with potential remedies for these issues. However, there is a significant research gap pertaining to the factors that might influence South African citizens to engage in cybersecurity practices.

Moreover, this chapter discussed existing literature on cybersecurity behaviours which included various international studies conducted within diverse contexts and employed different theoretical frameworks. Based on the literature discussed, several influential factors affecting cybersecurity Behavioural Intentions were identified, with the PMT and the TPB emerging as the most frequently utilised frameworks.

Chapter 3 Methodology

3.1 Introduction

This chapter will provide a discussion of the research methodology employed in this study. Chapter three details the theoretical underpinnings that form the basis of this study and the hypotheses derived from those theories. Research strategy, sampling methodology, data collection procedures used, research instrument, data analysis and ethical considerations will also be discussed in this chapter. Lastly, the methods used to investigate the factors that influence an individual's behavioural intention towards practising good cybersecurity behaviours will be elucidated.

3.2 Theoretical framework

A combination of two theoretical frameworks formed the basis of this study. The frameworks are the TPB, developed by Ajzen (1991) and the Protection Motivation Theory (PMT), developed by Rogers (1975), and revised by Maddux & Rogers (Maddux & Rogers, 1983; Rogers, 1975). The TPB endeavours to predict human behaviour (Ajzen, 1991), while the PMT aims to explore the factor of fear appeals influencing attitude and behaviour (Broer & Seydel, 1996). These two theories were combined in this study to gain more in-depth insight into the factors that could influence study participants' compliance with cybersecurity behaviour recommendations.

A study on the sufficiency of TPB in explaining security compliance found that the addition of the threat appraisal process of PMT improves the overall results of a security compliance study (Ifinedo, 2012; Sommestad et al., 2014b). Therefore, a combination of the constructs from TPB and PMT was used in this study to identify the factors that could influence an individual's cybersecurity behaviours. The dependent variable in this study is the Behavioural Intention, which refers to the practise of good cybersecurity behaviours. The hypotheses set out in this study aimed to test the degree to which the independent variables affect the dependent variable. An overview of the two theories is presented in sections 3.2.1 and 3.2.2.

3.2.1 Theory of planned behaviour

The TPB uses constructs to theorise that an individual's Behavioural Intention is shaped and influenced by the individual's Attitude to the behaviour, the Subjective norm and the Perceived behavioural control (Ajzen, 1991). The TPB consists of four constructs shown in Figure 3-1 below and discussed in sections 3.2.1.1 to 3.2.1.4.

3.2.1.1 Behavioural Intention

In TPB, Behavioural Intention refers to the factors that motivate and influence a certain behaviour (Ajzen, 1991). Behavioural Intention relates to the extent to which an individual is willing to try to do the action or behaviour (Ajzen, 1991). The theory states that a user's Behavioural Intention is influenced by three key factors, including Subjective norms, Attitude towards the behaviour and Perceived behavioural control (Aurigemma, 2013). For this study, Behavioural Intention refers to an individual's intent to try and perform good cybersecurity behaviours. Measuring an individual's actual cybersecurity behaviour is challenging (Crossler et al., 2013; Pham et al., 2017), and therefore the focus is mainly on an individual's self-reported Behavioural Intentions. TPB states that the stronger an individual's intention to perform that the behaviour is, the more likely they will actually perform the behaviour (Ajzen, 1991). Researchers like de Bruijn & Janssen (2017), Siponen et al. (2010), Sommestad et al. (2014b) and Yoon & Kim (2013) agree with Azjen (1991) that Behavioural Intention has a substantial impact on actual behavioural adoption. This study's approach required the inclusion of this construct in the in the South African context because its goal was to examine and understand the factors that influence South Africans' cybersecurity practices. The dependent variable employed to measure the practise of good cybersecurity behaviours among South Africans was Behavioural Intention.

3.2.1.2 Attitude towards the behaviour

This construct refers to whether an individual evaluates or appraises the behaviour as positive or negative and whether they see it as favourable or unfavourable to themselves (Ajzen, 1991). In this study, Attitude towards the behaviour refers to whether an individual views the practice of good cybersecurity behaviours in a positive or negative light. Within the South African context, the incorporation of this construct was integral to the framework of this study as South African's attitude towards the practise of good cybersecurity behaviours can help provide valuable insight into their intentions and actions related to cybersecurity behaviour. South Africans' perspectives on cybersecurity may be affected by elements unique to their culture, history, and social norms. Therefore, it is essential to take into consideration the cultural nuances that could affect attitude and in turn behaviour. Totest a user's Attitude towards good cybersecurity behaviours, the following hypothesis was formulated:

- H1: There is a positive association between an individual's Attitude towards good cybersecurity behaviours and the intention to practise good cybersecurity behaviours.

3.2.1.3 Subjective norm

Subjective norm is the social factor of the TPB. It refers to an individual's perception of whether society agrees or disagrees with performing the behaviour and the perceived pressure from society to perform the behaviour or not (Ajzen, 1991). An individual's Behavioural Intention is influenced by the people who are important to them and their opinion of performing the behaviour (Zhang et al., 2009). In this research study, the Subjective norm refers to cybersecurity awareness and how loved ones and society view the practice of good cybersecurity behaviours. Incorporating the construct Subjective norms into this research model in the South African context is not only theoretically sound but also practically relevant. It enables a thorough investigation of the sociocultural elements affecting cybersecurity behaviours in South Africa. This inclusion can aid policymakers, organisations, and educators in developing cybersecurity strategies that resonate with the social fabric of South Africa, ultimately promoting better cybersecurity practices. By examining Subjective norms, this research model can uncover cultural nuances and highlight the impact of these norms on South Africans' cybersecurity behaviours. Subjective norms can provide insight into what behaviour is considered socially acceptable or not in the context of cybersecurity, which is vital for developing effective educational and awareness campaigns. To test the subjective norm towards good cybersecurity behaviours, the following hypothesis was formulated:

- H2: There is a positive association between Subjective norms and an individual's intention to practice good cybersecurity behaviours.

3.2.1.4 Perceived behavioural control

This construct refers to how an individual's behaviour is heavily influenced by how confident they are in their ability to perform that behaviour (Ajzen, 1991). Perceived behavioural control refers to an individual's perception of the ease or difficulty of practising cybersecurity behaviours (Pham et al., 2017). Perceived behavioural control also relates to the Self-efficacy construct of PMT, which is the extent to which an individual has the capacity and necessary resources to execute the behaviour or action (Pham et al., 2017). TPB states that Perceived behavioural control and Behavioural intention can be used to predict actual behaviour (Ajzen, 1991).

In this study, Perceived behavioural control refers to an individual's cybersecurity knowledge and resources that might enable them to practise good cybersecurity behaviours. In the context of South Africa, where cybersecurity knowledge, skills, and resources vary widely, it is crucial to gauge people's confidence in their capacity to practice good cybersecurity behaviours. Understanding the effect of Perceived behavioural control / Self-efficacy can reveal empowerment or disempowerment factors, contributing to a nuanced understanding of cybersecurity behaviour. The construct of Perceived behavioural control / Self-efficacy highlights the importance of an individual's agency, showing that even those with limited knowledge, skills and resources can still engage in good cybersecurity behaviours if they believe in their capabilities. It enriches this study by considering the empowerment of individuals and the individual-level factors that contribute to good cybersecurity practices. Including this construct can aid in the development of tailored cybersecurity strategies to enhance Perceived behavioural control / Self-efficacy and, consequently, improve cybersecurity behaviours in South Africa. Therefore, this study will examine an individual's Perceived behavioural control's influence on behavioural intention, which is indicative of an individual's actual behaviour. Thus, the third hypothesis for this study is derived:

- H3: Self-efficacy / Perceived behavioural control will have a positive influence on an individual's behavioural intention to practice good cybersecurity behaviours.

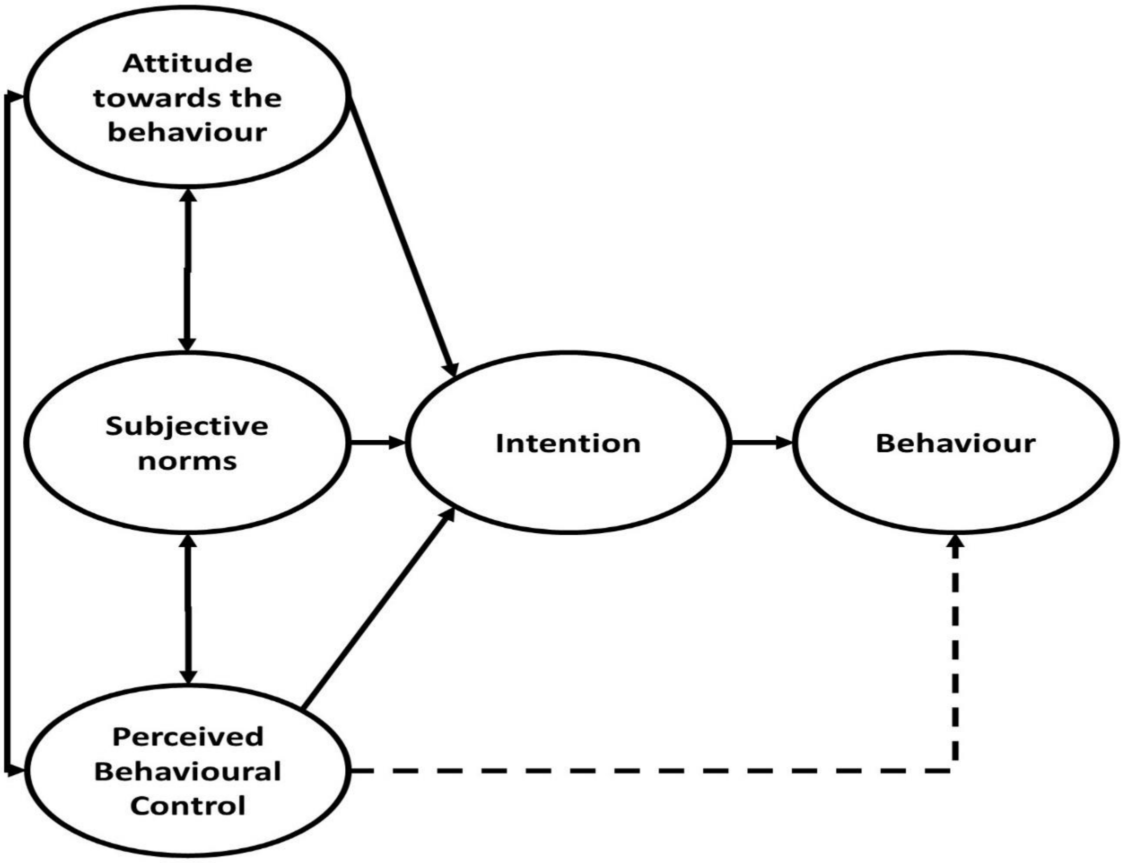


Figure 3-1 Theory of Planned Behaviour Source: Adapted from Aizen (1991:182)

Figure 3-1 above illustrates a visual model of the constructs of TPB and the relationships that exist between the constructs. TPB hypothesises that with the right attitude, combined with an appropriate level of perceived societal pressure to perform the behaviour and a high level of Self-efficacy / Perceived behavioural control should result in a more definite intention to carry out the particular behaviour (Ajzen, 1991; Aurigemma, 2013). In the context of this study, these factors were used to investigate the level of influence they have on an individual's intention to practise good cybersecurity behaviours.

3.2.2 Protection motivation theory

The PMT aims to explain how an individual is driven to respond to fear appeals, meaning warnings about threats or risky behaviours (Vance et al., 2012). When an individual receives a message in the form of a warning, they utilise a cognitive reasoning process to assess their response to the threat (Vance et al., 2012).

Cognitive reasoning is first concerned with the severity of the threat and the probability of the threat occurring; these two factors are an individual's threat appraisal (Maddux & Rogers, 1983). Threat appraisal is concerned with the threat's source and the level of danger it poses to the individual (Ifinedo, 2012). The next part of the individual's cognitive reasoning is the individual's perceived ability and capacity to perform the suggested coping response or behaviour (Maddux & Rogers, 1983). Coping appraisal focuses on an individual's coping responses available to address or mitigate the threat (Broer & Seydel, 1996). The PMT consists of four constructs shown in Figure 3-2 below, and is discussed in sections 3.2.2.1 to 3.2.2.4.

3.2.2.1 Perceived vulnerability and severity

Perceived vulnerability refers to an individual's evaluation of the likelihood of a threatening event occurring (Ifinedo, 2012). For this study, Perceived vulnerability is an individual's evaluation of whether they could become a victim of cyberthreats or cyberattacks. Perceived severity refers to an individual's assessment of the severity of the impact of a threat event occurring (Ifinedo, 2012). In this study, Perceived severity relates to an individual's understanding of the consequences of being a victim of a cyberattack or cyberthreat. If an individual views cyberattacks as a danger to themselves, with a high likelihood of occurrence and detrimental after-effects, the fear appraisal process will mediate their Perceived severity of a cyberthreat.

In South Africa, understanding people's perception of their vulnerability to cyberthreats and the severity of the potential consequences is essential. If South Africans perceive themselves as vulnerable to cyberthreats and believe the consequences of cyberattacks are severe, they are more likely to engage in good cybersecurity behaviours. Different communities and cultures within South Africa may have varying perceptions of vulnerability and severity related to cybersecurity. Including these constructs in the research model, allows this study to account for cultural nuances that may affect good cybersecurity behaviour as well as providing more insight into why some people take cybersecurity seriously while others do not. By knowing the degree to which individuals perceive vulnerability and severity, tailored messages and interventions can be used to address specific concerns and misconceptions about cybersecurity and cybersecurity behaviours.

These constructs then form the basis of the next hypotheses in this study:

- H4: Perceived vulnerability will have a positive influence on an individual's intention to practise good cybersecurity behaviours.
- H5: Perceived severity will have a positive influence on an individual's intention to practise good cybersecurity behaviours.
- H6: Perceived severity will mediate an individual's Perceived vulnerability and their intention to practise good cybersecurity behaviours.

3.2.2.2 Response efficacy

Response efficacy refers to an individual's perception of the benefits that could accrue from performing the recommended behaviour (Ifinedo, 2012). Response efficacy can be viewed as an outcome expectancy. This means that the belief that performing the recommended behaviour, as opposed to the current behaviour, will help remediate the threat event (Maddux & Rogers, 1983). Response efficacy is one of PMT's coping appraisal responses that state when an individual perceives a cyberthreat, they should adjust their behaviour to perform the recommended behaviour to avoid the consequences of a cyberthreat. This construct helps evaluate whether people believe that adopting these practices can effectively mitigate cyber threats and risks. If South Africans perceive that the recommended cybersecurity practices are effective, they are more likely to take those actions. Including this construct helps to uncover what drives people to practice good cybersecurity behaviours and can contribute to a deeper understanding of their intentions and behaviours. Response efficacy can highlight whether individuals from different social, cultural, and economic groups believe that they can effectively practise good cybersecurity behaviours. This insight can serve as a guide for policymakers, organisations, and educators in developing strategies that not only raise awareness but also emphasize the effectiveness of protection measures.

Thus, the construct of Response efficacy is used to form the following hypothesis of this study:

- H7: Response efficacy is positively associated with an individual's behavioural intention to practise good cybersecurity behaviours.

3.2.2.3 Response cost

Response cost refers to an individual’s perceived opportunity costs exhausted when performing the suggested behaviour (Ifinedo, 2012). These can be actual monetary or non-monetary costs associated with performing the recommended behaviour (Ifinedo, 2012). Response costs can be barriers that prevent an individual from performing the recommended behaviour, for example, a lack of resources (Broer & Seydel, 1996). In this study, Response costs refer to any monetary or non-monetary barriers that might be experienced when practising good cybersecurity behaviour. Response cost is a crucial component of the cost-benefit analysis that individuals perform when deciding whether to adopt certain behaviours, including cybersecurity practices. South Africa exhibits a wide range of socioeconomic disparities, due to these disparities different groups of the population may experience varying costs related to cybersecurity practices and behaviours. Therefore, understanding the costs associated with practicing good cybersecurity behaviours in South Africa is vital. It is essential to understand the specific Response costs that South Africans connect with good cybersecurity behaviours in order to identify potential barriers to practising these behaviours. By identifying these obstacles, businesses and policymakers can create targeted interventions to alleviate them and promote better cybersecurity behaviours. By taking into account not just the perceived advantages but also the actual costs and challenges people encounter, the inclusion of Response cost in this study model helps to provide a comprehensive assessment of the factors influencing people's practice of good cybersecurity behaviours.

These response costs can inhibit an individual’s intent to perform good cybersecurity behaviours; therefore, the next hypothesis in this study is:

- H8: Response costs associated with good cybersecurity behaviour will have a negative effect on an individual’s intention to practice good cybersecurity behaviours.

3.2.2.4 Self-efficacy

Self-efficacy refers to the extent to which an individual believes that they are capable enough, and have enough capacity and the necessary resources to perform the recommended behaviour or action (Ifinedo, 2012). In this study, Self-efficacy refers to cybersecurity knowledge and resources, which will determine whether an individual has the capacity to practise good cybersecurity behaviours. Changes in Self-efficacy, which translate to increased cybersecurity knowledge and resources in an individual, should result in increased behavioural intent and might influence the recommended behavioural changes (Maddux & Rogers, 1983). This construct of PMT is also represented in the TPB but is referred to as Perceived behavioural control (Sommestad et al., 2014b). Thus, Perceived behavioural control and Self-efficacy are used to form the H3 of this study, but will be referred to as Self-efficacy from this point onwards.

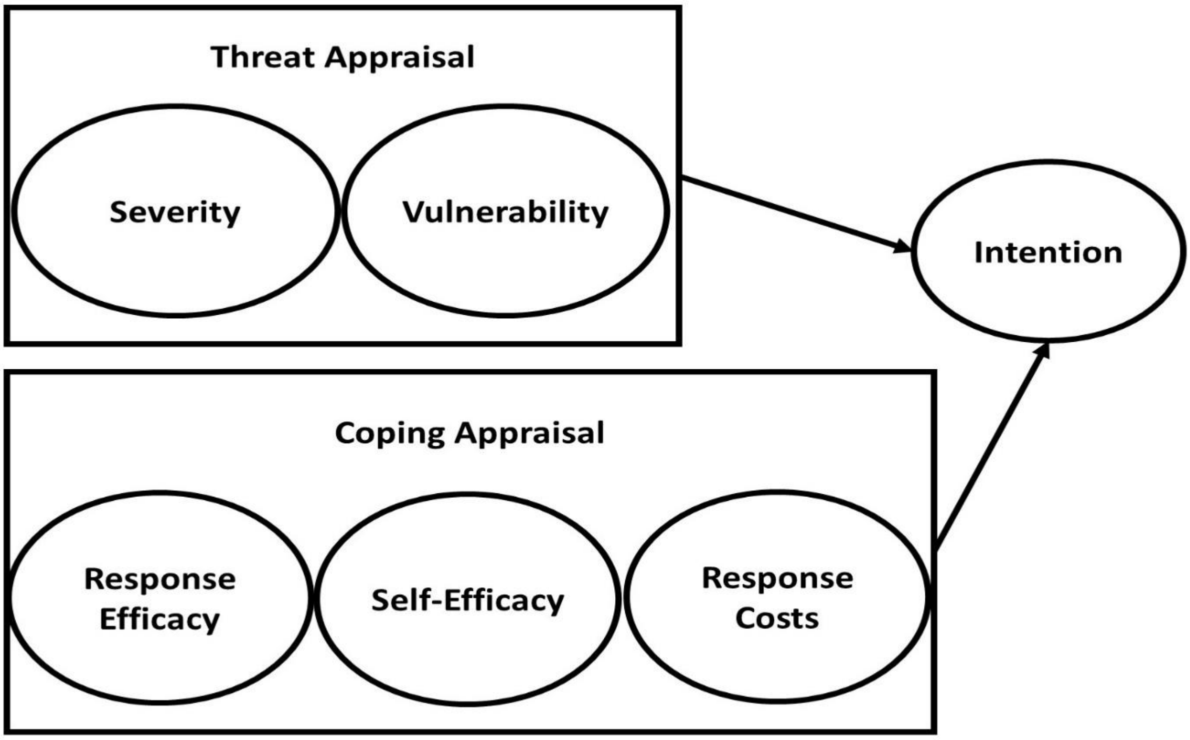


Figure 3-2 Protection Motivation Theory Source: Adapted from Maddux and Rogers (1983)

Figure 3-2 above illustrates a visual model of the constructs of PMT and the relationships that exist between the constructs. PMT hypothesises that an individual who can appraise the threat level and probability of a threat, combined with the effectiveness of the individual's coping response should result in higher intentions to carry out preventative behaviours (Maddux & Rogers, 1983). In the context of this study, these factors are combined with the TPB factors to investigate the level of influence they have on an individual's intention to practise good cybersecurity behaviours.

3.2.3 Covariates

This study included the personal characteristics of the respondents as these might be factors that influence an individual's intention to practise good cybersecurity behaviour (Zhang et al., 2009). The factors included level of education and time spent on the Internet (hours per day).

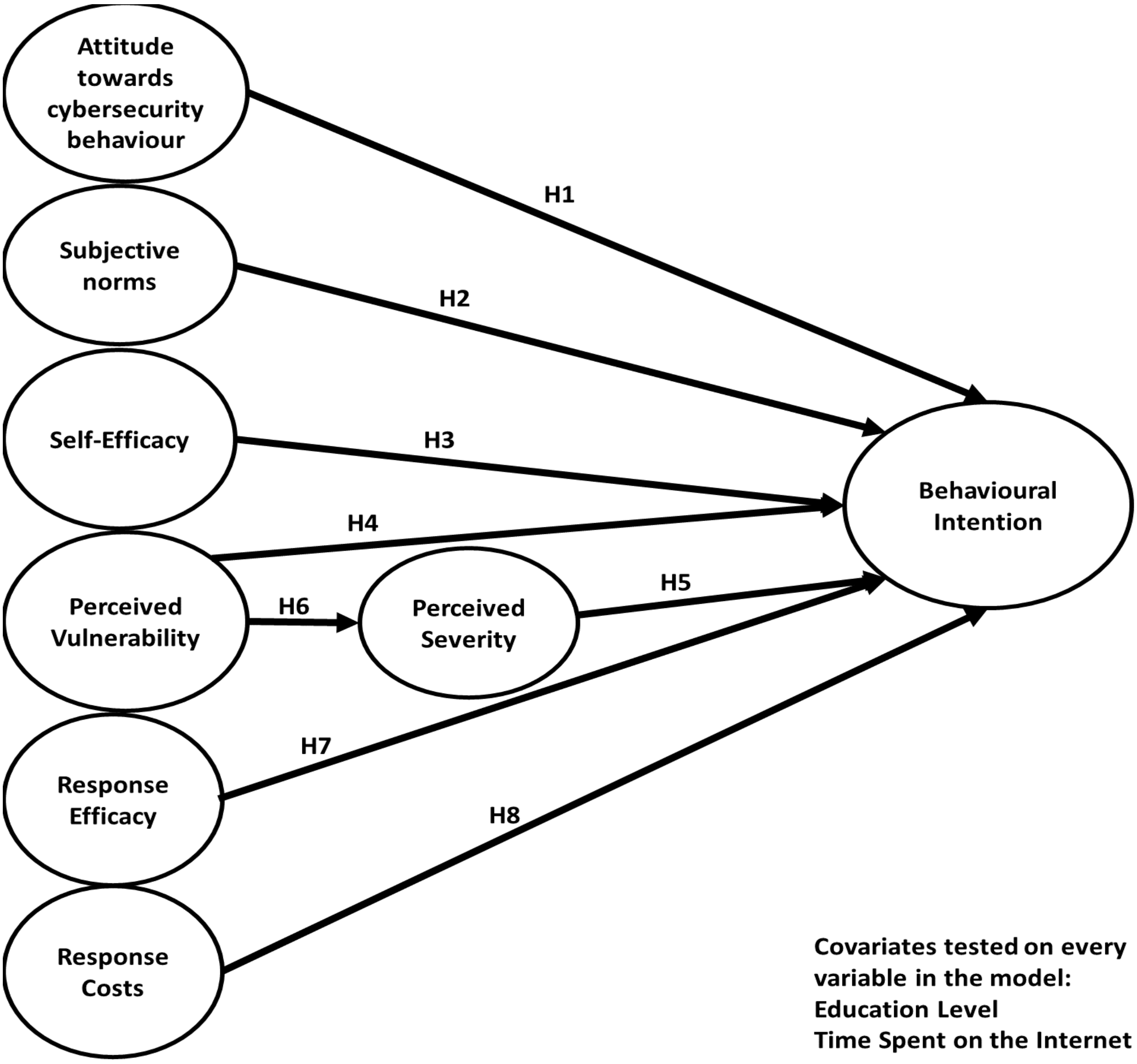


Figure 3-3 Proposed research model Source: Researcher's own

Figure 3-3 above illustrates the proposed research model used for this study based on a combination of the constructs of TPB and PMT.

3.3 Research strategy

There are many different research strategies that a researcher could employ while embarking on a study. These different research strategies could include design research, experiments, surveys, case studies, action research or ethnography.

This study aimed to use the data gathered to determine the factors that could influence the study participants to comply with cybersecurity behavioural recommendations and infer the findings to the larger population of South African Internet users. A survey is a widely used research method that involves collecting data from a sample of individuals to gather information about their attitudes, opinions, beliefs, behaviours, or characteristics (Oates, 2006). Surveys are typically conducted using structured questionnaires or interviews and are designed to gather quantitative or qualitative data, depending on the research objectives (Oates, 2006). The use of surveys is better suited to quantitative data analysis, which is the analysis methodology that is used in this study (Oates, 2006). Surveys are easily replicated and repeatable, which means that this study will be able to be repeated and tested again in the future, with other factors included. Surveys can be completed via the Internet (Oates, 2006), which is imperative for this study, as the COVID-19 pandemic limited in-person contact.

The survey strategy was employed in this study as it is the most suitable way to collect data from the sample. This strategy was chosen because it was necessary to collect data in a standardised way from a large group of respondents, which is an advantage of surveys as a research strategy (Oates, 2006). The survey data gathered could then be used to identify patterns in the surveyed group that could be postulated to larger population groups (Oates, 2006).

3.4 Sampling

This study aims to investigate the factors that influence good cybersecurity behaviour in South Africa. Therefore, the target population for this study is South African Internet users.

Two sampling methods are commonly used in research studies, namely probability sampling and non-probability sampling. Probability sampling is when the sample is chosen with the help of a probabilistic tool (Fricker, 2008), and there is a high chance that the sample chosen is illustrative of the total population (Oates, 2006), whereas non-probability sampling is used when the researcher is unsure as to whether the chosen sample is illustrative of the whole population (Oates, 2006). Non-probability sampling can be referred to as convenience sampling, as this method is used when there is no probabilistic tool to help, and respondents are selected because it is convenient for the researcher (Fricker, 2008). The non-probabilistic sampling method was used in this study, since in this study it is not possible to know the probability with which every person in the sample frame population could have been selected into the chosen sample (Fricker, 2008). In this study, the aim is to select respondents who are Internet users in South Africa to infer a generalisation about South African Internet users' cybersecurity behaviour. For this reason, the type of non-probability method that is used in this study is judgement sampling, which is a form of convenience sampling where the researcher uses their judgement to select the sample.

Multi-modal recruitment strategies are discussed in a study by McRobert, Hill, Smale, Hay & van der Windt (2018). The authors explored the use of multiple recruitment methods using traditional methods, social media and the Internet when sampling clinicians. The study made use of traditional methods (email, flyers, verbal) to drive people to the website link. They also made use of Twitter, Facebook, Google, LinkedIn and other online sources. Furthermore, the study demonstrated that it is possible to successfully recruit and sample a mixed sample group through the use of multi-modal recruitment strategies (McRobert et al., 2018).

For this study, the use of multi-modal recruitment strategies was employed to broaden and diversify the respondent sample. Multi-modal recruitment strategies enabled this study to have a mix of respondents with different professions, education levels, age groups and other demographic information (McRobert et al., 2018). The different methods used in this study included:

- Email invitation.
- Online message boards.
- Other Internet approaches (WhatsApp).
- Social media (Facebook, Twitter, Instagram, LinkedIn, blogs).

These multi-modal methods have the advantages of being moderate effort, lower cost, faster survey delivery and faster survey responses (McRobert et al., 2018). The use of social media sites enabled this current study to have a much broader potential reach. It enabled the researcher to use already existing social media connections and enabled easier sharing with those outside their network (McRobert et al., 2018). The use of social media added to the benefit of the chance of a snowballing effect (McRobert et al., 2018), which means respondents shared the questionnaire link with other potential participants. This study opted for a broad focus and did not target specific groups like IT security professionals or students because the aim was to obtain an accurate representation of general Internet users in South Africa.

3.5 Data collection procedure

For this study, questionnaires were used to collect data. These questionnaires were Internet-based and self-administered by the participants in this study. The use of Internet-based data collection enabled the collection of data from a wider range of respondents in a short amount of time (Oates, 2006). The target respondents were Internet users residing in South African and were easily sourced by using an Internet questionnaire, as respondents needed to use and access the Internet to participate (Oates, 2006). An advantage of using Internet surveys to administer the questionnaire was that the results were in an electronic format, which made processing and analysing the data quicker and easier (Oates, 2006). Questionnaires are best used in cases like the one investigated in this study because data needs to be gathered from a large number of people (Oates, 2006). The questionnaires were web-based to ensure that respondents did not receive an extensive, text-heavy email-based questionnaire (Oates, 2006).

For this study, quantitative data was generated using surveys. Quantitative data collection was chosen for this study due to the general scientific acceptance of this kind of data in the scientific community (Oates, 2006), as well as the fact that quantitative data analysis is based on recognised and established techniques (Oates, 2006). Quantitative data is measurable and logical as opposed to subjective qualitative data, and this type of data enables the researcher to analyse greater volumes faster using software (Oates, 2006).

Multi-modal methods were used to distribute the survey questionnaire link. Mainly using email invitations, online message boards, WhatsApp and multiple forms of social media (Facebook, Twitter, Instagram, LinkedIn and blogs). The online survey questionnaire used in this study was implemented in a survey tool called Qualtrics, provided by the University of Pretoria. The questionnaire responses were directly captured into the Qualtrics online software The data collection process took place between 1 February 2022 and 15 March 2022. At the end of the data collection process, the captured responses were exported from Qualtrics into Microsoft Excel. The Excel data file was then imported into Statistical Package for the Social Sciences (SPSS) software version 28 for data analysis.

3.6 Research instrument

The questionnaire used in this study quantitatively measured eight factors, namely: Behavioural Intention, Attitude towards good cybersecurity behaviour, Subjective norms, Self-efficacy, Perceived severity, Perceived vulnerability, Response efficacy, and Response cost. Under each construct, there were multiple questionnaire items, which were developed and guided by previous studies. A five-point Likert scale was utilised in this study's questionnaire, where one meant strongly disagree, and five meant strongly agree.

Table 3-1 below contains the measurement items and Cronbach's alpha score for each factor in this study, derived from previous studies that were used to guide the questions used in this study. The Cronbach's alpha score is used to assess the internal consistency or reliability of the constructs (Schumacker & Lomax, 2004). A construct is considered reliable if the Cronbach's alpha score is above 0.70 (Hair, Ringle & Sarstedt, 2013). For this study, the measurement items from previous studies were used, but the wording was changed slightly to match the objectives of this study.

Table 3-1 Items used in questionnaires from previous studies

Factor	Items	Definition	Source	Cronbach
Attitude towards good cybersecurity behaviour	Att1	Security measures such as implementing antivirus software, firewalls, or system updates on your home computer are a good idea	(Anderson & Agarwal, 2010)	0.88
	Att2	Taking security measures to protect your home computer is important		
	Att3	I like the idea of taking security measures to secure my home computer		
Behavioural intention	BehInt1	I intend to periodically use anti-spyware applications to protect my computer from spyware.	(Dinev & Hu, 2007)	0.83
	BehInt2	In the immediate future, I intend to customise my browser and computer settings to prevent the intrusion of spyware to my computer.		
	BehInt3	I intend to periodically check my browser and computer settings to prevent the intrusion of spyware to my computer.		
Self-efficacy	SelfE1	For me, taking information security precautions is: Hard . . . easy	(Workman, Bommer & Straub, 2008)	0.93
	SelfE2	I have the necessary skills to protect myself from information security violations: Disagree . . . agree		
	SelfE3	I have the skills to implement the available preventative measures to stop people from getting my confidential information: Disagree . . . agree		
	SelfE4	I have the skills to implement the available preventative measures to stop people from damaging my system: Disagree . . . agree		
	SelfE5	My skills required to stop information security violations are: Inadequate . . . adequate		
Subjective norm	Subj1	Most people who are important to me think it is a good idea to clean spyware from my computers.	(Dinev & Hu, 2007)	0.86
	Subj2	Most people who are important to me think it is a good idea to prevent spyware from running on my computer.		
Perceived severity	PSev1	I believe that protecting my confidential information is: Unimportant . . . important	(Workman et al., 2008)	0.97
	PSev2	Threats to the security of my confidential information are: Harmless . . . severe		
	PSev3	Having my confidential information accessed by someone without my consent or knowledge is: Harmless . . . severe		
	PSev4	Having someone successfully attack and damage my system is: Harmless . . . severe		

Factor	Items	Definition	Source	Cronbach
	PSev5	In terms of information security violations, [attacks on my information systems and equipment] are: Harmless . . . severe		
Perceived vulnerability	PVul1	The vulnerability of my confidential information to security violations is: Invulnerable . . . vulnerable	(Workman et al., 2008)	0.85
	Pvul2	I believe that trying to protect my confidential information will reduce illegal access to it: Unlikely . . . likely		
	Pvul3	The likelihood of someone getting my confidential information without my consent or knowledge is: Unlikely . . . likely		
	Pvul4	The likelihood of someone damaging my system is: Unlikely . . . likely		
	Pvul5	The likelihood of an information security violation occurring to me is: Unlikely . . . likely		
Response efficacy	RespE1	Efforts to keep my confidential information safe are: Ineffective . . . effective	(Workman et al., 2008)	0.91
	RespE2	The effectiveness of available measures to protect my confidential information from security violations is: Ineffective . . . effective		
	RespE3	The preventative measures available to me to stop people from getting my confidential information are: Inadequate . . . adequate		
	RespE4	The preventative measures available to me to stop people from damaging my system are: Inadequate . . . adequate		
	RespE5	The preventative measures available to keep people from violating information security are: Inadequate . . . adequate		
Response cost	RespC1	The inconvenience to implement recommended security measures: exceeds benefits . . . outweighed by benefits	(Workman et al., 2008)	0.79
	RespC2	The cost to implement recommended security measures: exceeds benefits . . . outweighed by benefits		
	Resp3	The impact to my work from recommended security measures: exceeds benefits . . . outweighed by benefits		

For the pre-testing stage of this study, the questionnaire items were initially reviewed by the study supervisor to determine content validity and relevance. A pilot study was conducted with a convenience sampling of 50 participants. The pilot questionnaire was shared via a uniform resource locator (URL) link to the pilot questionnaire configured in Qualtrics. This pilot test was conducted to test the usability and clarity of the questionnaire. This helped determine whether the questionnaire needed any modification for the participants to understand the instructions and content of the questionnaire thoroughly. The pilot test results revealed a need for minor changes in language and word choice for clarity. The final research questionnaire used in this dissertation can be found in Appendix B.

3.7 Data analysis

This study made use of statistical analysis techniques using Statistical Package for the Social Sciences (SPSS) software version 28 and IBM SPSS AMOS 28 Graphics to analyse the data collected from the survey.

Table 3-2 below indicates the coding that was used for the descriptive statistics. Descriptive statistics are commonly used to contextualise and summarise a study's data set (Field, 2013). The multivariate analysis of variance (MANOVA) test was used to identify any relationships between the descriptive statistic variables and the factors that might influence South African good cybersecurity Behavioural Intention. The statistical analysis techniques chosen for this study were MANOVA, Confirmatory factor analysis (CFA) and Structural Equation Modelling (SEM).

Table 3-2 Descriptive statistics coding

Variables	SPSS Variable Name	Coding Instrument
Highest Level of Qualification	Education	1 - Matric 2 - Undergraduate (Diploma) 3 - Undergraduate (Bachelor's degree) 4 - Postgraduate (Honours degree) 5 - Postgraduate (Master's degree) 6 - Postgraduate (PhD degree) 7 - Others (Please specify)
Do you currently live in South Africa	Resident	Yes No
Time spent on the Internet	TimeSpent	1 - Less than 2 Hours per day 2 - 2-4 Hours per day 3 - 4-8 Hours per day 4 - More than 8 Hours per day

3.8 Ethical considerations

Research ethics refers to the guidelines that ensure that the research is conducted responsibly and ethically, that must be used by a researcher when conducting their research (Oates, 2006). This research was conducted in line with the University of Pretoria’s Code of Ethics for Research (University of Pretoria, 2007). Ethical clearance was obtained from the University of Pretoria’s Faculty of Economic and Management Sciences Research Ethics Committee to ensure compliance (University of Pretoria, 2007). A copy of the ethics clearance is available in Appendix A.

The questionnaire used in this study did not ask the participants for any personally identifiable information like identity numbers or names. All participants were required to give their consent to participate in this study and could withdraw their consent by exiting the survey at any point. The survey was completed anonymously by respondents, and their privacy and anonymity were held to the highest standard. The researcher has an ethical responsibility to not encroach unnecessarily on participants, to act with integrity, not to plagiarise and to adhere to an ethical code of conduct (Oates, 2006).

3.9 Conclusion

This chapter aimed to detail in-depth the theoretical framework used in this study. This study utilised a combination of the TPB and PMT to identify and measure the constructs that affect a South African's intention to practise good cybersecurity behaviour. The research strategy, sampling method, data collection procedures and research instrument were outlined in this chapter. Lastly, this chapter outlined the data analysis techniques that were used and the ethical considerations that were taken into account.

Chapter 4 Analysis of findings

4.1 Introduction

This study aimed to identify the factors that have the most significant impact on a South African's intention to practise good cybersecurity behaviours. The factors measured in this study were: Attitude towards good cybersecurity behaviour, Behavioural Intention, Subjective norms, Perceived vulnerability, Perceived severity, Self-efficacy, Response efficacy and Response cost. The factors were analysed using MANOVA, CFA and SEM. The software IBM SPSS and IBM SPSS AMOS were used to analyse the data. Chapter 4 presents the results of the analysis of the data collected through the questionnaires.

4.2 Data screening

As discussed in section 3.5, an online questionnaire was used to collect data. The set-up of the online questionnaire on Qualtrics ensured that participants who were not comfortable responding to all items on the questionnaire could exit the survey at any stage. This ensured that there was no missing data in the records.

A total of 352 responses were received through the online questionnaire. After the data had been collected and entered into Microsoft Excel, empty rows due to formatting and unnecessary headers were removed. The data was then imported into SPSS, and the variable names and characteristics were defined. The data then went through the screening and cleaning phase, where steps were taken to ensure the correctness and cleanliness of the data to prepare for data analysis. Screening the data involved checking each of the variables for errors and out-of-range scores (Pallant, 2011), which was done by checking the Frequencies option and the minimum and maximum values for each variable in SPSS. No missing values or out-of-range entries were found in the data due to each question being mandatory in the questionnaire and the use of a Likert scale.

Two participants' responses were removed because they were minors in high school, and a further 21 responses were removed because the respondents were not currently residents of South Africa. This left 329 responses that were included in the final analysis. Table 4-1 below illustrates the education level of the questionnaire respondents. The majority of the respondents had an educational level of Undergraduate Bachelor's degree (83 respondents). Table 4-2 below describes the time spent on the Internet by the respondents. The majority of the respondents indicated that they spend between four and eight hours a day (119 respondents), followed by more than eight hours a day on the Internet (111 respondents). The effect of these variables on good cybersecurity Behavioural Intention was analysed using the MANOVA method. The analysis and discussion of the effect of education level and time spent on the Internet are provided in section 4.5.

Table 4-1 Respondents' education level

Variable	Item	Number of respondents	Percentage
Education Level	Matric	66	20.1
	Undergraduate (Diploma)	47	14.3
	Undergraduate (Bachelor's degree)	83	25.2
	Postgraduate (Honours degree)	78	23.7
	Postgraduate (Master's degree)	39	11.9
	Postgraduate (PhD degree)	6	1.8
	Other (mainly certificates)	10	3

Table 4-2 Respondents' time spent on the Internet

Variable	Item	Number of respondents	Percentage
Time spent on the Internet	Less than 2 Hours per day	14	4.3
	2-4 Hours per day	85	25.8
	4-8 Hours per day	119	36.2
	More than 8 Hours per day	111	33.7

4.2.1 Outliers

Outliers are cases where respondents' responses are substantially different from the others in a set of data (Byrne, 2010). A discrete Likert scale from one to five was used in the questionnaire for this study. The Mahalanobis distance, which is usually used to identify outliers in responses does not apply to discrete data as the questionnaire data collected using Likert scales are not multivariate normally distributed (Zijlstra, 2009). Due to the statement above, visual analysis was conducted using the boxplots and stem and leaf plots for the residuals of the composite variables in the dataset using IBM SPSS. The visual analysis showed no extreme outliers for the dataset. Therefore, there were no outliers in the data used for this study.

4.2.2 Assessing normality

The data was assessed for normality of distribution by checking the skewness and kurtosis values for the factors in the model. The factors were transformed into new target factors by taking the mean of all the items in each factor (Boone & Boone, 2012; Pallant, 2011; Tabachnick & Fidell, 2013). Kurtosis measures the peakedness of a distribution, while skewness measures the asymmetry of the distribution of the different data variables. For skewness, values between -3 and 3 are considered normally distributed (Brown, 2006; Dhir, Yossatorn, Kaur & Chen, 2018). For kurtosis, values between -10 and 10 are considered normally peaked enough to use in factor analysis (Brown, 2006; Collier, 2020). The skewness and kurtosis values for the composite variables are shown in Table 4-3 below. All the values fall within the acceptable threshold. Therefore, the data can be considered normally distributed enough to continue with CFA.

Table 4-3 Normality test table

Variable	Measure	Value	Std. Error
TotAttitude	Skewness	-2.18	0.13
	Kurtosis	7.44	0.27
TotBehInt	Skewness	-0.72	0.13
	Kurtosis	0.36	0.27
TotSubj	Skewness	-0.64	0.13
	Kurtosis	-0.10	0.27
TotPVul	Skewness	0.01	0.13
	Kurtosis	-0.60	0.27
TotPSev	Skewness	-0.81	0.13
	Kurtosis	0.17	0.27
TotRespE	Skewness	-0.49	0.13
	Kurtosis	0.25	0.27
TotSelfE	Skewness	-0.84	0.13
	Kurtosis	1.28	0.27
TotRespC	Skewness	0.31	0.13
	Kurtosis	-0.59	0.27

TotAttitude: The scale total for the Attitude towards good cybersecurity behaviours measurement items.
TotBehInt: The scale total for the Behavioural Intention measurement items
TotSubj: The scale total for the Subjective Norms measurement items
TotPVul: The scale total for the Perceived Vulnerability measurement items
TotPSev: The scale total for the Perceived Severity measurement items
TotRespE: The scale total for the Response Efficacy measurement items
TotSelfE: The scale total for the Self-efficacy measurement items
TotRespC: The scale total for the Response Cost measurement items

The Central Limit Theorem states that if the sample sizes are sufficiently large (n > 30), the means of samples will be normally distributed regardless of the distributions of the population (Kwak & Kim, 2017; Tabachnick & Fidell, 2013). Therefore, univariate normality was not tested due to the large sample size of this study. It can be assumed, according to the Central Limit Theorem, that the underlying data is approximately normally distributed (Kwak & Kim, 2017; Tabachnick & Fidell, 2013).

4.2.3 Correlation and factor loadings

The Kaiser-Meyer-Olkin measure of sampling adequacy (KMO) and the Bartlett test of sphericity were used to determine the suitableness of the data for factor analysis. The acceptable criteria for the KMO test are values above 0.50. The closer a value is to one, the more suitable the data is for factor analysis (Shrestha, 2021; Silva, Sabino, Lanuza, Adina, Villaverde & Pena, 2014). As seen in Table 4-4 below, the KMO value for the data was 0.83, which indicates that the criteria of sampling adequacy were met for this dataset.

Bartlett's test of sphericity was performed to determine the suitability of the data for factor analysis. Bartlett's test of sphericity is used to evaluate whether the correlation matrix of the variables is significantly different from an identity matrix, indicating whether the variables are sufficiently intercorrelated for factor analysis (Shrestha, 2021). The Bartlett's test of sphericity was statistically significant (*p* = 0.000) for the dataset used in this study.

Table 4-4 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.83
Bartlett's Test of Sphericity	Approximate Pearson's chi-squared	5324.93
	Degrees of Freedom	465
	Significance	0.000

An initial factor analysis was performed on the 21 measurement items from the questionnaire, using IBM SPSS. The extraction method used was Maximum Likelihood and the rotation method used was Varimax with Kaiser Normalization. The rotated factor matrix shows the item loadings on the different factors (Pallant, 2011). The initial rotated factor matrix indicated that some of the items were cross-loading on different factors. The items that were cross-loading (BehInt1, PVul2, PSev1, PSev2, SelfE1, RespE1) were removed one at a time. The rotated factor matric was checked after each item was removed to check if there were still items that were cross-loading.

The analysis was repeated to achieve the results illustrated in Table 4-5 below. Table 4-5 below shows the final item loadings for the factors used in this study. All items showed strong loadings on a single factor, except for one item which cross-loaded (SelfE5). However, the item loaded strongly enough on its own factor to be included in the further analysis (Pallant, 2011; Schumacker & Lomax, 2004). The eight-factor model explained 66.2% variance of the total variance of the model. The total variance is a measure of how well the extracted factors capture the variance in the observed variables (Tabachnick & Fidell, 2013). Higher total variance values are considered more desirable, as they indicate that the extracted factors account for a larger portion of the variance in the observed variables (Hair, Black, Babin & Anderson, 2010).

Table 4-5 Rotated factor matrix

	Factor							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Att1				0.72				
Att2				0.89				
Att3				0.72				
BehInt2								0.96
BehInt3								0.60
Subj1							0.71	
Subj2							0.98	
PVul1			0.58					
PVul3			0.74					
PVul4			0.79					
PVul5			0.83					
PSev3						0.44		
PSev4						0.89		
PSev5						0.73		
SelfE2		0.76						
SelfE3		0.84						
SelfE4		0.74						
SelfE5	0.32	0.71						
RespE2	0.58							
RespE3	0.82							
RespE4	0.80							
RespE5	0.83							
RespC1					0.71			
RespC2					0.83			
RespC3					0.83			
Only showing the coefficients greater than 0.30								

4.3 Confirmatory factor analysis

4.3.1 Model testing

Using SPSS AMOS, CFA was then conducted on the dataset. The extraction method used was Maximum Likelihood. The model was assessed and tested for reliability, convergent validity, and discriminant validity. Figure 4-1 below illustrates the first model created in AMOS, which shows the interaction between the latent, observed variables and standardised factor loading values for each item and relationship. The first model, shown in Figure 4-1 below, was used to evaluate the model fit measures to test the suitability of the proposed model. The following model fit measures were assessed: Pearson's chi-squared test / degrees of freedom (CMIN/df), the Goodness-of-Fit Index (GFI), Comparative Fit Index (CFI), Standardised Root Mean Square (SRMR) and Root Mean Square Error of Approximation (RMSEA). The acceptable values for each model fit measure are shown in Table 4-6 below. As shown in Table 4-6 below, the initial CFA eight-factor model yielded an acceptable fit for the measurement values: CMIN/df = 1.72, GFI= 0.91, CFI= 0.96, SRMR= 0.04, and RMSEA= 0.05.

Table 4-6 Initial CFA model fit indices

Fit Indices	**Obtained Value**	**Recommended Value**	**References**	**Model fit outcome**
CMIN/df	1.73	<5	(Marsh & Hocevar, 1985; Schumacker & Lomax, 2004; Wheaton, Muthén, Alwin & Summers, 1977)	Good
GFI	0.91	>0.90	(Byrne, 2010; Hair et al., 2010)	Acceptable
CFI	0.96	>0.90	(Bentler, 1990; Byrne, 2010; Schumacker & Lomax, 2004)	Acceptable
SRMR	0.04	<0.08	(Hu & Bentler, 1998; Kline & St, 2022)	Good
RMSEA	0.05	<0.10	(Browne & Cudeck, 1992; Fabrigar, Wegener, MacCallum & Strahan, 1999; Weston, P. A. & Catalano, 2008)	Good
CMIN/df: Pearson's chi-squared test / degrees of freedom GFI: Goodness-of-Fit Index CFI Comparative Fit Index SRMR: Standardised Root Mean Square RMSEA: Root Mean Square Error of Approximation				

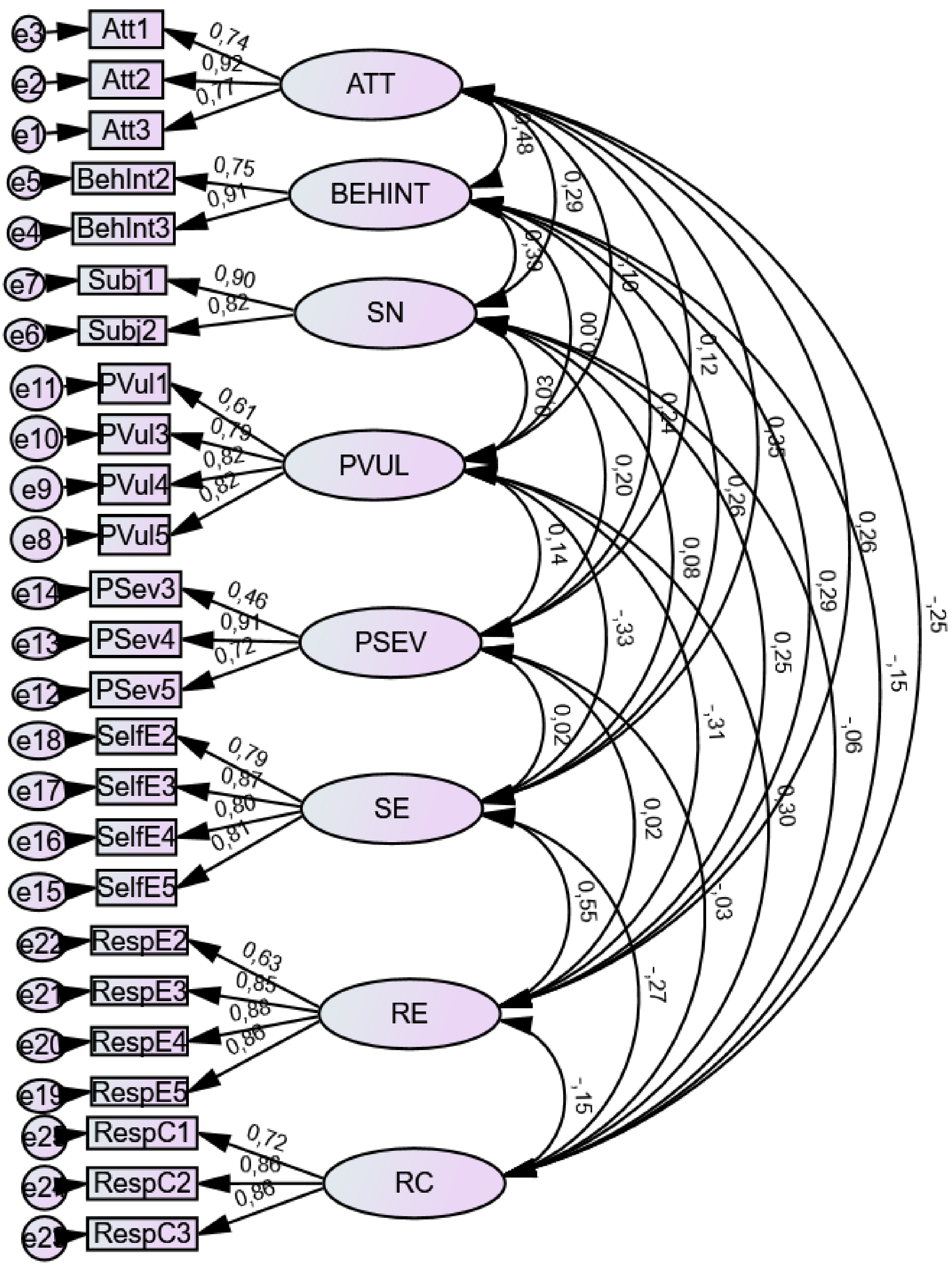


Figure 4-1 Initial CFA model Source: Researcher's own using IBM SPSS AMOS 28

Though the initial CFA model revealed an acceptable model fit, one measurement item had a low standardised factor loading (PSev3<0.50), which can be seen in Figure 4-1 above. Due to this low factor loading item, further modifications to the model were made. The item was removed from the model due to low factor loading (DeVellis, 2012). The CFA model analysis was repeated to obtain the results shown below in Table 4-7 and Figure 4-2.

The final model revealed a good model fit. The CMIN/df = 1.74, GFI = 0.91, CFI = 0.96, SRMR = 0.04, and RMSEA = 0.05 (see Table 4-7 below). The factor loadings, illustrated in Figure 4-2 below, ranged between 0.63 and 0.92. The results of the fit indices tested met the criteria for the recommended acceptable values of a model with a good fit.

Table 4-7 Final CFA model fit indices

Fit Indices	Obtained Value	Recommended Value	References	Model fit outcome
CMIN/df	1.74	<5	(Marsh & Hocevar, 1985; Schumacker & Lomax, 2004; Wheaton et al., 1977)	Good
GFI	0.91	>0.90	(Byrne, 2010; Hair et al., 2010)	Acceptable
CFI	0.96	>0.90	(Bentler, 1990; Byrne, 2010; Schumacker & Lomax, 2004)	Good
SRMR	0.04	<0.08	(Hu & Bentler, 1998; Kline & St, 2022)	Good
RMSEA	0.05	<0.10	(Browne & Cudeck, 1992; Fabrigar et al., 1999; Weston et al., 2008)	Good
CMIN/df: Pearson's chi-squared test / degrees of freedom GFI: Goodness-of-Fit Index CFI Comparative Fit Index SRMR: Standardised Root Mean Square RMSEA: Root Mean Square Error of Approximation				

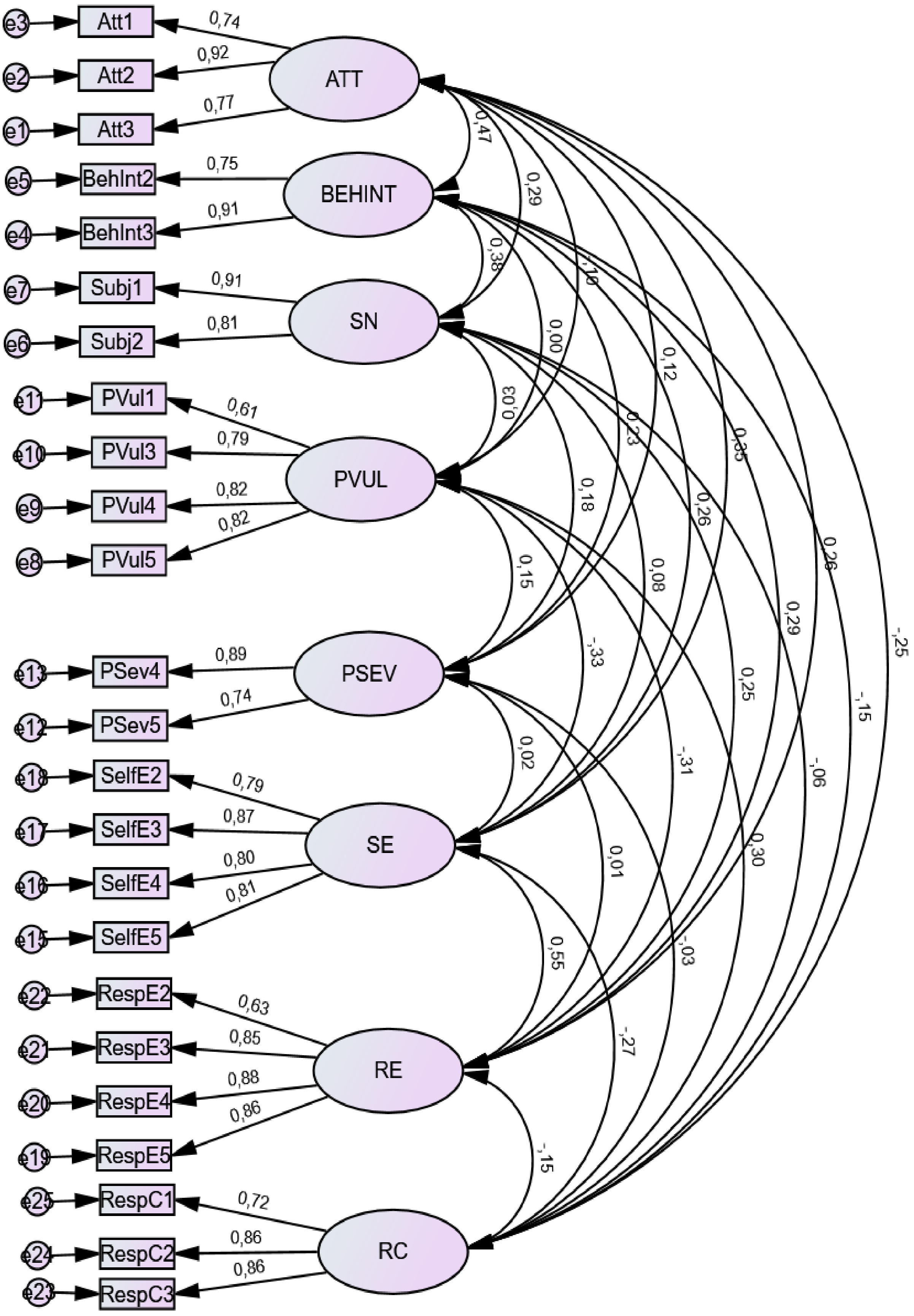


Figure 4-2 Final CFA model Source: Researcher's own using IBM SPSS AMOS 28

4.3.2 Construct reliability of final model

Before proceeding with SEM analysis, the reliability and validity of the constructs in the final model were assessed (Schumacker & Lomax, 2004). Reliability is the measure of the internal consistency of the constructs in the data (Schumacker & Lomax, 2004). To assess the internal consistency of the items in the final model, the Cronbach's alpha of the items was calculated. A construct is considered reliable if the Cronbach's alpha score is above 0.70 (Hair et al., 2013).

Table 4-8 below shows the results of the construct reliability. All constructs were found to be reliable. Composite reliability (CR) was also assessed. Composite reliability is "an indicator of the shared variance amongst the observed variables used as an indicator of a latent construct" (Fornell & Larcker, 1981). As shown in Table 4-8 below, the composite reliability values of the variables in this study ranged from 0.80 to 0.89. A higher CR value indicates higher reliability (Ab Hamid, Samil & Sidek, 2017). The recommended benchmark value for CR is a value above 0.70 (Ab Hamid et al., 2017; Clark & Watson, 1995; DeVellis, 2012; Nunnally & Bernstein, 1994). Therefore, construct reliability was established for each proposed factor in the study.

Table 4-8 Reliability and convergent validity table

Variables/ Constructs	Items	Std Factor Loadings	Cronbach’s Alpha	Composite Reliability	Avg Variance Extracted	Max Shared Variance
Attitude towards good cybersecurity behaviour	Att1	0.74	0.85	0.86	0.67	0.23
	Att2	0.92				
	Att3	0.77				
Behavioural Intention	BehInt2	0.75	0.81	0.82	0.70	0.23
	BehInt3	0.91				
Subjective norms	Subj1	0.91	0.85	0.85	0.74	0.15
	Subj2	0.81				
Perceived vulnerability	PVul1	0.61	0.84	0.85	0.58	0.11
	PVul3	0.79				
	PVul4	0.82				
	PVul5	0.82				
Perceived severity	PSev4	0.89	0.78	0.80	0.67	0.05
	PSev5	0.74				
Self-efficacy	SelfE2	0.79	0.89	0.89	0.67	0.30
	SelfE3	0.87				
	SelfE4	0.80				
	SelfE5	0.81				
Response efficacy	RespE2	0.63	0.88	0.88	0.66	0.30
	RespE3	0.85				
	RespE4	0.88				
	RespE5	0.86				
Response cost	RespC1	0.72	0.85	0.85	0.62	0.09
	RespC2	0.86				
	RespC3	0.86				
Model Fitness: X2 = 392.05, df = 225, X2/df = 1.74, RMSEA = 0.05, RMR = 0.04, SRMR = 0.04 GFI = 0.91, CFI = 0.96						

4.3.3 Convergent validity

The convergent validity of the scale items in the final model was calculated using the Average Variance Extracted (AVE) (Fornell & Larcker, 1981). As shown in Table 4-8 above, the AVE values for all the constructs were above the recommended threshold of 0.50 (Ab Hamid et al., 2017; Bagozzi & Yi, 1988; Fornell & Larcker, 1981). Comparing the Maximum Shared Variance (MSV) to the AVE for each variable is another commonly used technique to determine convergent validity. In this case, when the MSV is less than the AVE for all variables, it indicates that the variables meet the test. Therefore, based on this criterion, the data satisfies the requirements for convergent validity.

4.3.4 Discriminant validity

Discriminant validity indicates the extent to which a given construct differs from other constructs (Anderson & Gerbing, 1988). Since there were multiple constructs measured in the current dataset, the constructs should have their own distinct identity and should not overlap. The Fornell & Larcker Criterion was used in this study (Fornell & Larcker, 1981; Henseler, Ringle & Sarstedt, 2015). According to the Fornell & Larcker Criterion, discriminant validity is established when the square root of the AVE for a construct is greater than its correlation with the other constructs (Fornell & Larcker, 1981). In Table 4-9 below, the highlighted values are the square root of the AVE. This value should be higher than the other values in its column. Thus, it can be said that the variables meet the criteria for good discriminant validity.

Table 4-9 Fornell and Larcker Criterion

	ATT	SN	PVUL	PSEV	SE	RE	RC	BEHINT
ATT	**0.82**							
SN	0.29	**0.86**						
PVUL	-0.10	0.03	**0.76**					
PSEV	0.12	0.18	0.15	**0.82**				
SE	0.35	0.08	-0.33	0.02	**0.82**			
RE	0.26	0.25	-0.31	0.01	0.55	**0.81**		
RC	-0.25	-0.06	0.30	-0.03	-0.27	-0.15	**0.81**	
BEHINT	0.47	0.38	-0.002	0.23	0.26	0.29	-0.15	**0.84**

ATT: Attitude towards good cybersecurity behaviour
SN: Subjective norms
PVUL: Perceived vulnerability
PSEV: Perceived severity
SE: Self-efficacy
RE: Response efficacy
RC: Response cost
BEHINT: Behavioural Intention

4.4 Full structural model analysis

4.4.1 Model identification and testing

A structural model analysis was created and analysed using SEM in SPSS AMOS, as shown in Figure 4-3 below. The model was used to assess the relationships between Behavioural Intention and Attitude towards good cybersecurity behaviour, Subjective norms, Perceived vulnerability, Perceived severity, Self-efficacy, Response efficacy and Response cost. Figure 4-3 below shows the proposed structural model that was used for SEM analysis. The factor scores from the CFA model were imputed using SPSS AMOS's Data Imputation function. Specifically, regression imputation was used to create the structural model depicted in Figure 4-3 below. As part of hypothesis testing, Perceived severity (PSEV) was tested as a mediator between Perceived vulnerability and Behavioural Intention.

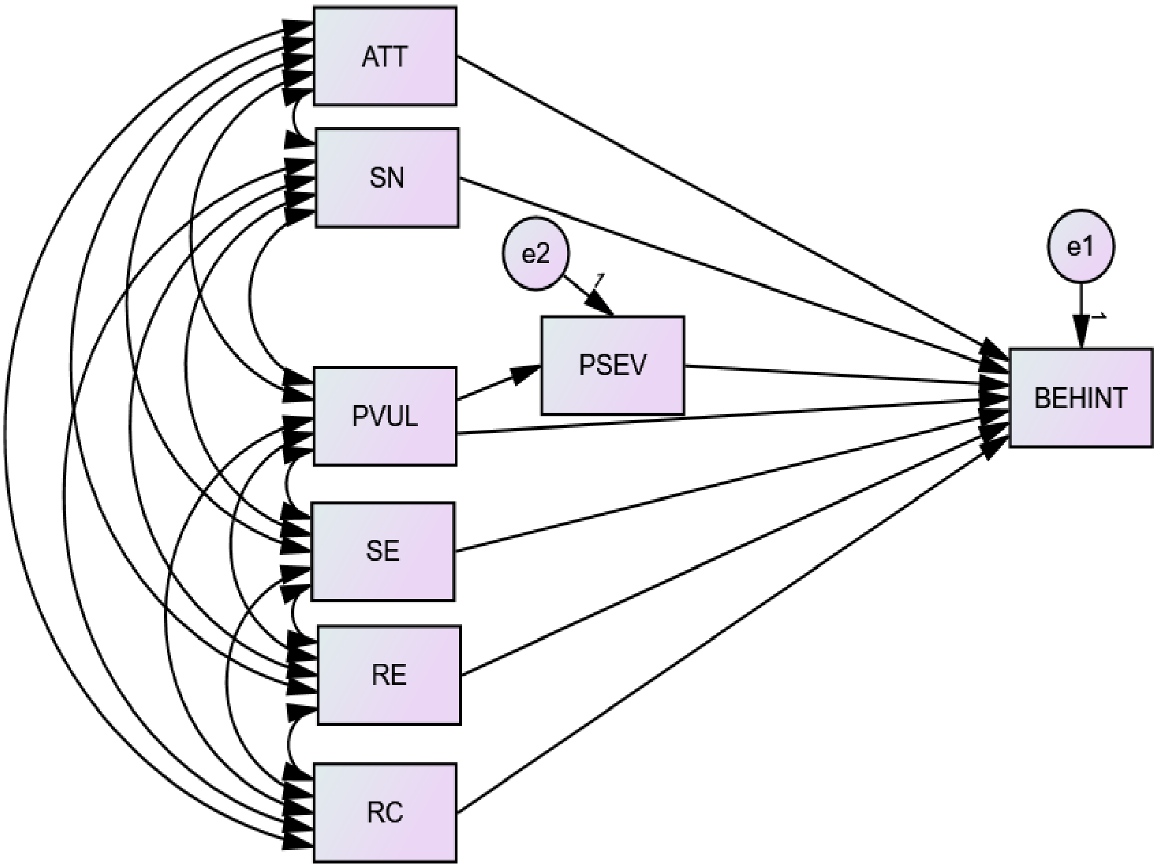


Figure 4-3 Proposed structural model for hypothesis testing Source: Researcher's own using IBM SPSS AMOS 28

4.4.2 Model estimation

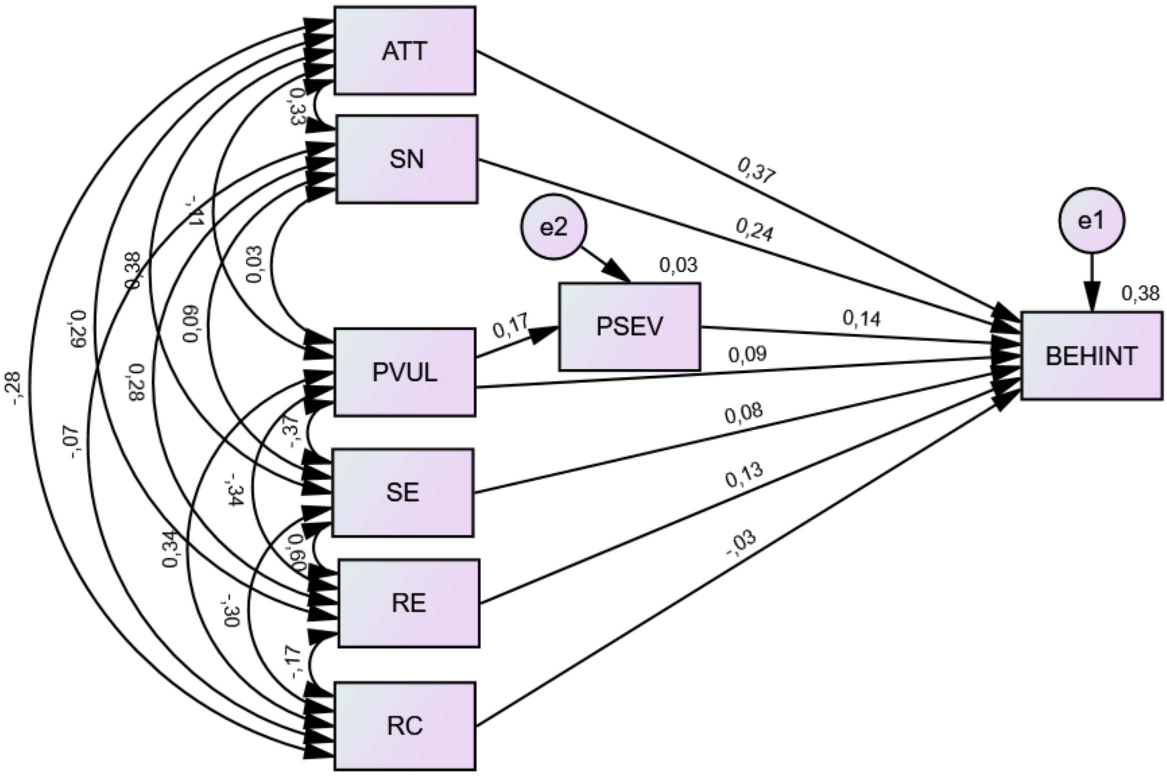


Figure 4-4 Final Research model Source: Researcher's own using IBM SPSS AMOS 28

Figure 4-4 above shows the resulting final model produced in AMOS with the path estimates. The extraction method used was the Maximum Likelihood method. The structural model estimated in AMOS revealed a good model fit (CMIN/df = 3.93, GFI = 0.99, CFI = 0.97, SRMR = 0.05, RMSEA = 0.10).

Figure 4-4 above also shows that the square multiple correlations (R^2) for Behavioural Intention was 0.38. This result indicates that 38% of the variance in Behavioural Intention was accounted for by the factors measured in this study (Attitude towards good cybersecurity behaviour, Subjective norms, Perceived vulnerability, Perceived severity, Self-efficacy, Response efficacy, and Response cost).

4.4.3 Sequential equation modelling path analysis

Table 4-10 below and Figure 4-4 above illustrate the results of the path estimates from the SEM analysis performed. As shown in Table 4-10 below, five of the hypothesised paths revealed significant results. Attitude towards good cybersecurity behaviour on

Behavioural Intention was significant and positive (β = 0.37, t = 7.38, *p* < 0.001). Subjective norms had a positive and significant impact on Behavioural Intention (β = 0.24, t = 5.03, *p* < 0.001). Perceived severity's effect on Behavioural Intention was positively significant (β = 0.14, t = 3.26, *p* = 0.001). Response efficacy on Behavioural Intention was positive and significant (β = 0.13, t = 2.27, *p* = 0.023). Perceived vulnerability's effect on Perceived severity was significant and positive (β = 0.17, t = 3.08, *p* = 0.002). Due to the significant relationship between Perceived severity and Perceived vulnerability, mediation testing was performed in section 4.4.4. The hypothesis results are further discussed in Chapter five.

Table 4-10 Hypothesis results

H.No.	**Path**	**Standardised Estimates (β)**	**t-value**	***p*-value**
H1	Attitude towards good cybersecurity behaviour-> Behavioural Intention	0.37	7.38	<0.001
H2	Subjective Norm -> Behavioural Intention	0.24	5.03	<0.001
H3	Perceived Vulnerability -> Behavioural Intention	0.09	1.74	0.08
H4	Perceived Severity -> Behavioural Intention	0.14	3.26	0.001
H5	Perceived Vulnerability -> Perceived Severity	0.17	3.08	0.002
H6	Self-Efficacy -> Behavioural Intention	0.08	1.30	0.19
H7	Response Efficacy -> Behavioural Intention	0.13	2.27	0.02
H8	Response Cost -> Behavioural Intention	-0.03	-0.55	0.58

4.4.4 Mediation testing

A mediation analysis was conducted where Behavioural Intention was the independent variable, Perceived vulnerability was the dependent variable and Perceived severity was the mediator. The Baron & Kenny (1986) approach to mediation analysis based on indirect effect was utilised to determine the effect of the mediator. Mediation analysis was conducted in SPSS AMOS. Using bootstrapping procedures (2 000 samples) and bias-corrected bootstrap confidence interval (90%) to determine the direct and indirect effects of Perceived severity as a mediator of Perceived vulnerability and Behavioural Intention. The results of the mediation analysis are shown in Table 4-11 below.

Table 4-11 Mediation analysis

Path	Direct Effects	Indirect Effects	Total Effects
Perceived vulnerability > Perceived severity > Behavioural Intention	0.09	0.02 **	0.11*

*<0.05 , **<0.001

The results of the mediation analysis show that Perceived severity partially mediates the relationship between Behavioural Intention and Perceived vulnerability since the indirect effect is statistically significant (β = 0.02, *p* < 0.001).

4.5 Effect of education level and time spent on the internet on Behavioural Intention

The effect of the descriptive statistics on a user's intention to practise good cybersecurity behaviours was analysed. MANOVA was used to determine if there are any differences in Behavioural Intention and education levels and time spent on the Internet existed.

MANOVA is a statistical technique that enables researchers to establish if a set of categorical predictor variables, that is, the independent variables (IV), can explain the variability in a set of continuous response variables, that is, the dependent variables (DV) (DeCoster & Claypool, 2004; Tabachnick & Fidell, 2013). MANOVA was chosen because there are multiple dependent variables in this study. Two separate MANOVA tests, instead of a two-way MANOVA, were run to analyse the effect of the IVs on the DVs. This was because this study's focus was not on the interaction effect between education level and time spent on the Internet but rather the differences in the separate groups' levels.

This study employed the use of a Likert scale in the questionnaire to collect data. To perform an analysis on the scale items they needed to be transformed into a composite score (Boone & Boone, 2012; Retutas & Rubio, 2021). In this study, the means of the scale items were used to determine the composite variables to be analysed (TotAttitude, TotBehInt, TotSubj, TotPVul, TotPSev, TotRespE, TotSelfE, TotRespC).

4.5.1 Multivariate analysis on the education level

Assumption testing

The assumptions for using a MANOVA were tested to ensure the data did not violate any of the assumptions. The assumption tests for MANOVA are as follows (French, Macedo, Poulsen, Waterson & Yu, 2008; Tabachnick & Fidell, 2013):

- The data is normally distributed.
- There is linearity in the data.
- There are no univariate or multivariate outliers in the data.
- There is homogeneity and equality of variance-covariances in the data.

The Central Limit Theorem states that if the sample sizes are sufficiently large (n > 50), the means of samples will be normally distributed regardless of the distributions of the population (Kwak & Kim, 2017; Tabachnick & Fidell, 2013). Due to the sample size (n = 329) of this study, univariate normality was not tested. It can be assumed, according to the Central Limit Theorem, that the underlying data is approximately normally distributed (Kwak & Kim, 2017; Tabachnick & Fidell, 2013). The data was tested for outliers and multivariate normality on the residuals of the composite variables, and no extreme values were found.

The linearity of the data was tested by visually analysing the scatter plot diagrams of the DVs and the IV in SPSS. The visual analysis revealed the relationships between the variables appear to be reasonably linear.

The Box's test of equality of covariance matrices (Box's M test) and Levene's test for equality of error variance (Levene's test) were utilised to determine the homogeneity and variance-covariance of the data. The Box's M test for education and the DVs was conducted (see Table 4-12 below) and revealed *p* = 0.02. Due to the large number of DVs and seven groups in the IV in the dataset that was analysed, the sample sizes across the groups were unequal. According to Tabachnick & Fidell (2013), the robustness of the Box M's test cannot be guaranteed if sample sizes are unequal, and the test revealed significant results at $p < 0.001$. However, the Box’s M test for this dataset showed non-significant results at $p > 0.001$. The Box’s M test requires a non-significant result for the assumption of homogeneity of variance-covariance matrices to be met (Hahs-Vaughn, 2016). Hahs-Vaughn (2016), Tabachnick & Fidell (2013), Field (2013) and Pituch & Stevens (2012) suggest using a more liberal alpha level of $p = 0.001$ for Box’s M test, as this test is known to be highly sensitive to sample size and unequal sample sizes across groups (Denis, 2020; Field, 2013; Hahs-Vaughn, 2016; Pituch & Stevens, 2012; Tabachnick & Fidell, 2013). Based on the suggestions of these authors, the dataset was deemed appropriate enough to proceed with the MANOVA test (Denis, 2020).

Table 4-12 Box's test of equality of covariance matrices

Test	**Value**
Box's M	255.92
F	1.24
df1	180
df2	8788.71
Sig. (*p*)	0.02

Box's M: Box’s M test value
F: Value on the F distribution
df1: Degrees of freedom 1
df2: Degrees of freedom 2
Sig. (p): Significance level (p-value)

The Levene’s test revealed non-significant results for all variables except for Attitude towards good cybersecurity behaviours, which revealed a significance value of $p = 0.008$. The value obtained was less than the benchmark alpha value used for this test of $p < 0.05$ (Field, 2013). Therefore, equality of variance was not established. Due to this violation, the Pillai trace test was utilised instead of Wilks’ Lambda, as it is known to be more robust against violations of the assumptions for MANOVA (DeCoster & Claypool, 2004; Pallant, 2011; Tabachnick & Fidell, 2013).

Multivariate Analysis test

The hypothesis for this MANOVA test was:

H9: There are significant differences between the different education levels and a user’s intention to practise good cybersecurity behaviours.

The results of the MANOVA test showed that there was a significant difference between the seven education level groups of the independent variable on the combined dependent variables (see Table 4-13 below). The different group levels are Matric, Undergraduate (Diploma), Undergraduate (Bachelor's degree), Postgraduate (Honours degree), Postgraduate (Master's degree), Postgraduate (PhD degree), and Other (mainly certificates). The Pillai's trace test results indicated significance, V = 0.21, F (48,1920) = 1.47, *p* = 0.02, partial eta squared = 0.04, observed power = 0.99. This result indicates that there are significant differences in the effect of education level and a user's intention to practise good cybersecurity behaviours. The effect size or partial eta squared refers to the proportion of variance of the DVs that is explained by the IVs (Pallant, 2011; Richardson, 2011). In this case, the effect size is large (partial eta squared = 0.35 or 35%). The observed power, in this case, was 0.99 or 99%.

Table 4-13 Education level MANOVA test result

Effect		**Value**	**F**	**Hypothesis df**	**Error df**	**Sig. (*p*)**	**Partial Eta Squared**	**Noncent. Parameter**	**Observed Power**
Education	Pillai's Trace	0.21	1.47	48	1920	**0.02**	0.04	70.42	0.99

F: Value on the F distribution
Hypothesis df: Hypothesis degrees of freedom
Error df: The number of degrees of freedom associated with the model errors.
Sig. (p): Significance level (p-value)
Partial Eta Squared: The proportion of variance of the DVs that is explained by the IVs
Noncent. Parameter: The degree of misspecification of the model
Observed Power: The statistical power of the test, based on the effect size estimate

Due to the MANOVA test results being significant, the test of between-subject effects, which are a series of subsequent one-way ANOVAs SPSS performs (see Table 4-14 below). Table 4-14 below shows the test of between-subject effects, which is used to determine how the DVs differ for the IV. The Bonferroni method was used to analyse the results of the multiple ANOVAs to protect against inflated Type 1 errors (Tabachnick & Fidell, 2013). The adjusted Bonferroni alpha value, in this case, is 0.05 / 8 = 0.00635. The results of the tests show that all the DVs revealed non-significant results at the alpha level *p* < 0.00635. The effect sizes ranged from low (partial eta squared = 0.01) to almost medium (partial eta squared = 0.05) (Richardson, 2011).

Table 4-14 Tests of between-subject effects MANOVA results

IV	**DV**	**Type III Sum of Squares**	**df**	**Mean Square**	**F**	**Sig. (*p*)**	**Partial Eta Squared**	**Observed Power**
Education	TotAtt	4.40	6	0.73	1.59	0.15	0.03	0.61
	TotBehInt	4.17	6	0.70	1.10	0.36	0.02	0.43
	TotSubj	2.34	6	0.39	0.48	0.82	0.01	0.20
	TotPVul	4.64	6	0.77	1.42	0.21	0.03	0.55
	TotPSev	6.27	6	1.05	2.59	0.02	0.05	0.85
	TotSelfE	2.52	6	0.42	1.01	0.42	0.02	0.40
	TotRespE	2.14	6	0.36	0.67	0.68	0.01	0.27
	TotRespC	13.00	6	2.17	2.11	0.05	0.04	0.76

TotAttitude: The scale total for the Attitude towards good cybersecurity behaviours questionnaire items.
TotBehInt: The scale total for the Behavioural Intention questionnaire items.
TotSubj: The scale total for the Subjective norms questionnaire items.
TotPVul: The scale total for the Perceived vulnerability questionnaire items.
TotPSev: The scale total for the Perceived severity questionnaire items.
TotRespE: The scale total for the Response efficacy questionnaire items.
TotSelfE: The scale total for the Self-efficacy questionnaire items.
TotRespC: The scale total for the Response cost questionnaire items.

Due to the conflicting results of the MANOVA and ANOVA tests, a post hoc analysis was performed on all the DVs (Chen, Xu, Tu, Wang & Niu, 2018). This test entails conducting pairwise comparisons to determine which education level affected the dependent variables the most (Chen et al., 2018; Ruxton & Beauchamp, 2008). The Games-Howell post hoc test was used to perform the post hoc analysis, as it is often used when there are unequal sample sizes or unequal variances (Field, 2013; Ruxton & Beauchamp, 2008). The Games-Howell post hoc test revealed non-significant results for all DVs at every group level.

Considering the results of the post hoc analysis, there is not enough evidence to prove the hypothesis. Therefore, the hypothesis is rejected, and it can be concluded that education level does not have any influence on a user's intention to practise good cybersecurity behaviours.

4.5.2 Multivariate analysis on time spent on the Internet

Assumption testing

The assumptions for using a MANOVA were tested in section 4.5.1. The Box's M test and Levene's test were used to determine the homogeneity and variance-covariance of the data. The Box M's test for time spent on the Internet and the DVs was conducted (see Table 4-15 below) and revealed p = 0.02. This value indicates non-significant results as p > 0.001. Due to the large number of DVs and seven groups in the IV in this dataset, the sample sizes across the groups were unequal. As discussed in section 4.5.1, Hahs-Vaughn (2016) and Tabachnick & Fidell (2013) suggest using a more liberal alpha level of p = 0.001 for Box's M test. That being considered, the dataset was deemed appropriate enough to proceed with the MANOVA (Denis, 2020).

Table 4-15 Box's test of equality of covariance matrices

Test	Value
Box's M	157.87
F	1.30
df1	108
df2	7406.26
Sig. (*p*)	0.02
Box's M: Box's M test value F: Value on the F distribution df1: Degrees of freedom 1 df2: Degrees of freedom 2 Sig. (p): Significance level (p-value)	

Levene's test revealed non-significant results for all variables except for Attitude towards good cybersecurity behaviours (p = 0.047) and Self-efficacy (p = 0.002), these values were less than the benchmark alpha value used for this test of p < 0.05 (Field, 2013). Therefore, equality of variance was not established. Due to this violation, the Pillai's trace test was utilised instead of Wilks' Lambda, as it is known to be more robust against violations of the assumptions for MANOVA (Pallant, 2011; Tabachnick & Fidell, 2013).

Multivariate Analysis test

The hypothesis for this MANOVA test was:

H10: There are significant differences between the different levels of time spent on the Internet and a user's intention to practise good cybersecurity behaviours.

The results of the MANOVA showed that there was a significant difference between the four levels of time spent on the Internet of the independent variable on the combined dependent variables (see Table 4-16 below). The different group levels are Less than two hours per day, 2-4 hours per day, 5-8 hours per day, and more than 8 hours per day.

The Pillai's trace test results were significant, V = 0.15, F (24,960) = 2.12, *p* = 0.001, partial eta squared = 0.50, observed power = 0.99. The results in Table 4-16 below, indicate that there are significant differences in the effect between the amount of time spent on the Internet and a user's intention to practise good cybersecurity behaviours. The effect size or partial eta squared refers to the proportion of variance of the DVs that is explained by the IVs (Pallant, 2011; Richardson, 2011). The effect size, in this case, is large (partial eta squared = 0.50 or 50%). The observed power, in this case, was 0.99 or 99%.

Table 4-16 MANOVA test results for time spent on the Internet

Effect		**Value**	**F**	**Hypothesis df**	**Error df**	**Sig. (*p*)**	**Partial Eta Squared**	**Noncent. Parameter**	**Observed Power**
Time Spent	Pillai's Trace	0.15	2.12	24	960	**0.001**	0.05	50.76	0.99

F: Value on the F distribution
Hypothesis df: Hypothesis degrees of freedom
Error df: The number of degrees of freedom associated with the model errors.
Sig. (p): Significance level (p-value)
Partial Eta Squared: The proportion of variance of the DVs that is explained by the IVs
Noncent. Parameter: The degree of misspecification of the model
Observed Power: The statistical power of the test, based on the effect size estimate

Table 4-17 Tests of between-subjects effects ANOVA test results

IV	**DV**	**Type III Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.** (*p*)	**Partial Eta Squared**	**Observed Power**
Time spent	TotAtt	5.57	3	1.86	4.10	0.007	0.04	0.85
	TotBehInt	8.47	3	2.82	4.60	**0.004**	0.04	0.89
	TotSubj	7.26	3	2.42	3.07	0.028	0.03	0.72
	TotPVul	2.85	3	0.95	1.74	0.158	0.02	0.45
	TotPSev	1.29	3	0.43	1.03	0.380	0.01	0.28
	TotSE	3.90	3	1.30	3.18	0.024	0.03	0.73
	TotRE	2.57	3	0.86	1.62	0.184	0.02	0.43
	TotRC	1.84	3	0.62	0.59	0.625	0.01	0.17

Due to the results of the MANOVA test being significant, there is a need to test each DV using the ANOVA method, to determine which variables were causing the significant MANOVA result. The Bonferroni method was utilised to determine the adjusted alpha value. The adjusted Bonferroni alpha value, in this case, is 0.05/8 = 0.00635. The results of the univariate tests revealed that there were significant results only for Behavioural Intention (*p* = 0.004). The effect sizes ranged from low (partial eta squared = 0.01) to almost medium (partial eta squared = 0.04) (Richardson, 2011). These results show that there is a difference in a user's behavioural intention to practise good cybersecurity behaviours and the time they spend on the Internet.

Post hoc analysis was performed on all the DVs by conducting pairwise comparisons to determine which time spent on the Internet group level affected the IV the most (Chen et al., 2018; Ruxton & Beauchamp, 2008). The Games-Howell post hoc test was used to perform the post hoc analysis as it is often used when there are unequal sample sizes or unequal variances (Field, 2013; Ruxton & Beauchamp, 2008), which was indicated by the failed Levene's test. The Games-Howell post hoc test with 95% bias-corrected confidence intervals on the mean differences revealed significant results at *p* < 0.05 for the different groups' comparisons across the dependent variables.

For DV = Attitude towards good cybersecurity behaviours

- Less than 2 hours vs. 2-4 hours: *p* < 0.001
- Less than 2 hours vs. 5-8 hours: *p* = 0.002
- Less than 2 hours vs. More than 8 hours: *p* = 0.02
- 2-4 hours vs. More than 8 hours: *p* = 0.04

For DV = Behavioural Intention

- Less than 2 hours vs. 2-4 hours: *p* < 0.001
- Less than 2 hours vs. 5-8 hours: *p* = 0.001
- Less than 2 hours vs. More than 8 hours: *p* = 0.02

For DV = Subjective norms

- Less than 2 hours vs. 5-8 hours: *p* = 0.01
- Less than 2 hours vs. More than 8 hours: *p* = 0.04

Table 4-18 Games-Howell results for time spent on the Internet (Only significant pairs shown)

DV	(I) Time Spent on Internet	(J) Time Spent on Internet	Mean Difference (I-J)	Std. Error	Sig. (*p*)	95% Confidence Interval	
						Lower Bound	Upper Bound
TotAtt	Less than 2 Hours per day	2-4 Hours per day	0.58	0.11	**<0.001**	0.28	0.87
		5-8 Hours per day	0.43	0.11	**0.002**	0.14	0.72
		More than 8 Hours per day	0.33	0.10	**0.02**	0.05	0.60
	2-4 Hours per day	Less than 2 Hours per day	-0.58	0.11	**<0.001**	-0.87	-0.28
		More than 8 Hours per day	-0.25	0.09	**0.04**	-0.49	-0.01
	5-8 Hours per day	Less than 2 Hours per day	-0.43	0.11	**0.002**	-0.72	-0.14
	More than 8 Hours per day	Less than 2 Hours per day	-0.33	0.10	**0.02**	-0.60	-0.05
		2-4 Hours per day	0.25	0.09	**0.04**	0.01	0.49
TotBehInt	Less than 2 Hours per day	2-4 Hours per day	0.75	0.16	**<0.001**	0.32	1.18
		5-8 Hours per day	0.65	0.15	**0.001**	0.23	1.07
		More than 8 Hours per day	0.49	0.15	**0.02**	0.08	0.90
	2-4 Hours per day	Less than 2 Hours per day	-0.75	0.16	**<0.001**	-1.18	-0.32
	5-8 Hours per day	Less than 2 Hours per day	-0.65	0.15	**0.001**	-1.07	-0.23
	More than 8 Hours per day	Less than 2 Hours per day	-0.49	0.15	**0.02**	-0.90	-0.08
TotSubj	Less than 2 Hours per day	5-8 Hours per day	0.69	0.19	**0.01**	0.17	1.21
		More than 8 Hours per day	0.55	0.18	**0.04**	0.03	1.06
	5-8 Hours per day	Less than 2 Hours per day	-0.69	0.19	**0.01**	-1.21	-0.17
	More than 8 Hours per day	Less than 2 Hours per day	-0.55	0.18	**0.04**	-1.06	-0.03

TotAttitude: The scale total for the Attitude towards good cybersecurity behaviours questionnaire items.
TotBehInt: The scale total for the Behavioural Intention questionnaire items.
TotSubj: The scale total for the Subjective norms questionnaire items.

Based on the results presented in Table 4-18 above, there is sufficient evidence to accept the hypothesis. These results showed that there is a difference in a user's behavioural intention and the time they spend on the Internet, specifically DV's Attitude towards good cybersecurity behaviour, Behavioural Intention and Subjective norms.

4.6 Conclusion

Chapter four of this research study provided a detailed description of the data screening, analysis, and results of the study. The data collected for the study was screened and analysed using IBM SPSS and SPSS AMOS software. CFA was performed in both software to ensure that the data, constructs, and proposed model were suitable for the use of SEM to determine the hypotheses path. The iterative process of CFA resulted in a model with good fit indices, indicating that the model accurately represented the data. Construct reliability, convergent validity, and discriminant validity were established in the final construct items, ensuring that the measures used to assess the constructs were reliable, valid, and distinct from each other.

The full structural model analysis was conducted to determine the relationship between the constructs and test the hypotheses. Six out of the eight hypotheses were supported by the data, indicating that Attitude towards good cybersecurity behaviours, Subjective norms, Perceived severity, and Response efficacy have significant effects on an individual's intention to practice good cybersecurity behaviours. Perceived severity was found to have a mediating effect on the relationship between Perceived vulnerability and intention to practice good cybersecurity behaviours.

Furthermore, MANOVA was performed in SPSS on the dataset. The purpose of this analysis was to test whether there were any significant differences in a user's intention to practice good cybersecurity behaviours based on their levels of education and time spent on the Internet. It was found that there were no significant differences across the education levels. However, there were significant differences in the levels of time spent on the Internet, suggesting that the amount of time spent on the Internet has an impact on a user's intention to practice good cybersecurity behaviours.

Chapter 5 General discussion of results and conclusion

5.1 Introduction

User behaviour is a prevalent area of interest in information security research (Almansoori et al., 2023). Understanding the factors that influence users' engagement in good cybersecurity behaviours is vital in contemporary times. This comprehension has the potential to enhance overall cybersecurity postures and effectively mitigate the consequences of cyberattacks. Therefore, this study focused on investigating the factors that influence South African citizens to practice good cybersecurity behaviours while online to protect themselves. Chapter five presents a general discussion of results and the conclusion of this study. This includes the summary of findings, implications for theory and practise and the conclusion.

5.2 Summary of findings

This study aimed to investigate the factors that influence good cybersecurity behavioural intention amongst South Africans and which factors have the most significant impact on behavioural intention. The results of the research model in this study (see Figure 4-4 in section 4.4.2) showed that 38% of the variance in Behavioural Intention was accounted for by the factors measured (Attitude towards good cybersecurity behaviour, Subjective norms, Perceived vulnerability, Perceived severity, Self-efficacy, Response efficacy, and Response cost). The hypotheses tested in this study were based on the theoretical frameworks of TPB and PMT. The results of the hypothesis testing are shown in Table 5-1 below.

Table 5-1 Summary of hypotheses

H.No.	Statement	Status
H1	There is a positive association between an individual's Attitude towards practising good cybersecurity behaviours and the intention to practise good cybersecurity behaviours.	Supported
H2	There is a positive association between Subjective norms and an individual's intention to practice good cybersecurity behaviours.	Supported
H3	Perceived vulnerability will have a positive influence on an individual's intention to practise good cybersecurity behaviours.	Not Supported
H4	Perceived severity will have a positive influence on an individual's intention to practise good cybersecurity behaviours	Supported
H5	Perceived severity will mediate an individual's Perceived vulnerability and the intention to practise good cybersecurity behaviours	Supported
H6	Increased cybersecurity Self-efficacy/Perceived behavioural control will have a positive influence on an individual's behavioural intent to practice good cybersecurity behaviours.	Not Supported
H7	Response efficacy is positively associated with an individual's behavioural intention to practise good cybersecurity behaviours	Supported
H8	Response costs associated with cybersecurity behaviour will have a negative effect on an individual's intention to practice good cybersecurity behaviours	Not Supported
H9	There are significant differences in the effect between education level and a user's intention to practise good cybersecurity behaviours	Not Supported
H10	There are significant differences in the effect between the level of time spent on the Internet and a user's intention to practise good cybersecurity behaviours.	Supported

The first research hypothesis examined whether a positive Attitude towards practising good cybersecurity behaviours would result in increased intention to practise good cybersecurity behaviours. The results shown in Table 4-10 (section 4.4.3) show the impact of Attitude towards practising good cybersecurity behaviours on Behavioural Intention was highly positive and significant (β = 0.37, t = 7.377, $p < 0.001$), where β is the path coefficient, and t is the critical ratio. The path coefficient (β = 0.37) indicates the strength of the relationship between Attitude towards practising good cybersecurity behaviours and Behavioural Intention. A positive coefficient suggests that there is a positive relationship between the two variables, meaning that as Attitude towards practising good cybersecurity behaviours increases, so does Behavioural Intention. The critical ratio (t = 7.377) indicates the level of statistical significance of the relationship between the two variables. The *p*-value ($p < 0.001$) indicates that this relationship is highly significant, meaning that it is unlikely to have occurred by chance. Thus, the first hypothesis is supported.

This result is consistent with the TPB, and other similar studies performed in an organisational context like Ifinedo (2012), and Siponen et al. (2013). This finding is similar to those of Aigbefo, Blount & Marrone (2020), Yoon & Kim (2013), Zhang et al. (2009), Foltz, Newkirk & Schwager (2016), Grimes & Marquardson (2019), Aderibigbe & Ocholla (2020); Farooq, Ndiege & Isoaho (2019).This finding suggests that having a positive attitude towards practising good cybersecurity behaviours is positively associated with the intention to practise those behaviours. In other words, people who have a positive attitude towards good cybersecurity behaviours are more likely to have the intention to engage in those behaviours than people who have a negative or neutral attitude.

The second hypothesis examined whether there is a positive association between Subjective norms (societal influence) and an individual’s intention to practice good cybersecurity behaviours. The results (see Table 4-10 in section 4.4.3) revealed that the effect of Subjective norms on Behavioural Intention was positive and highly significant ($\beta = 0.24$, $t = 5.03$, $p < 0.001$), supporting H2. This is consistent with TPB and other studies utilising the theory in an IS behaviour context like Ifinedo (2012), Foltz et al. (2016), Grimes & Marquardson (2019), Aderibigbe & Ocholla (2020); Farooq et al. (2019), Siponen, Mahmood & Pahnila (2014).

One study by Siponen et al. (2014) investigated the factors that influence employees' intention to comply with information security policies in organisations. The study found that Subjective norms, along with Self-efficacy, Perceived severity, Perceived vulnerability, and Attitude, had a significant positive effect on the intention to comply with information security policies. A study by Ifinedo (2012) found that Subjective norms were positively associated with security Behavioural Intention, suggesting that organisational culture can influence employees' intentions to practice good cybersecurity behaviours.

Overall, these studies provide support for the idea that Subjective norms can have a positive impact on individuals' intentions to practice good cybersecurity behaviours. By considering the social and cultural factors that influence individuals' attitudes and behaviours towards cybersecurity, organisations can develop more effective strategies to improve overall cybersecurity awareness and practices This finding supports the expectation that an individual’s intention to practise good cybersecurity behaviours is influenced by society and the people who are important to the individual. This means that perceived societal pressure can positively influence an individual to practise good cybersecurity behaviours.

The third hypothesis of this study posited that Perceived vulnerability would have a positive influence on an individual’s intention to practise good cybersecurity behaviours. The analysis of data (see Table 4-10 in section 4.4.3) revealed that the effect of Perceived vulnerability on Behavioural Intention was positive but not very significant ($\beta = 0.09$, $t = 1.74$, $p = 0.08$). Due to this, H3 was not supported. Perceived vulnerability looks at measuring an individual’s perceived probability that a threat exists. This finding implies that an increase in an individual’s Perceived vulnerability to a cybersecurity threat does not increase their intention to practise good cybersecurity behaviours.

This result is not consistent with the proposition of PMT, but other studies have found similar results in the IS domain like Johnston & Warkentin (2010), Vance et al. (2012) and Mills & Sahi (2019). A similar study by Farooq et al. (2019) on factors affecting the security behaviour of Kenyan students, found similar results on the non-effect of perceived vulnerability on behavioural intentions.

Overall, previous studies suggest that the relationship between Perceived vulnerability and intention to practice good cybersecurity behaviours may not always be straightforward. While some studies have found a positive relationship between Perceived vulnerability and intention to practice good cybersecurity behaviours (Ifinedo, 2012; Siponen et al., 2014; Workman et al., 2008), other studies have found no significant relationship or a more complex relationship (Johnston & Warkentin, 2010; Mills & Sahi, 2019; Vance et al., 2012; Yoon, Hwang & Kim, 2012). Factors such as individual differences and situational factors may play a role in shaping this relationship.

The fourth hypothesis of this study aimed to investigate whether Perceived severity would have a positive influence on an individual's intention to practice good cybersecurity behaviours. Perceived severity refers to an individual's perception of the seriousness and magnitude of a cyberthreat and the extent to which they believe that damage would occur if they were the victim of a cybersecurity event. The results of the analysis (see Table 4-10 in section 4.4.3) showed that the effect of Perceived severity on Behavioural Intention was highly positive and significant ($\beta = 0.14$, $t = 3.26$, $p = 0.001$), thus supporting H4.

This finding suggests that individuals who perceive cyberthreats as severe are more likely to engage in good cybersecurity behaviours. This finding is consistent with PMT and other previous studies in the field. For instance, Crossler & Bélanger (2014) tested their Unified Security Practices instrument and found that Perceived severity was a significant predictor of good cybersecurity Behavioural Intention. Similarly, Yoon et al. (2012), Siponen et al. (2013), and Vance et al. (2012) found that Perceived severity was positively associated with intention to practice good cybersecurity behaviours.

Overall, these findings suggest that the Perceived severity of a cybersecurity threat is an important factor in predicting an individual's intention to practice good cybersecurity behaviours. Organisations and policymakers can leverage this information to design interventions that emphasise the severity of cybersecurity threats to motivate individuals to engage in more secure online behaviours.

The fifth hypothesis posited that Perceived severity mediates an individual's Perceived vulnerability and Behavioural Intention. Though H3 found that the influence of Perceived vulnerability on Behavioural Intention was not significant, the mediation test results (see Table 4-11 in section 4.4.4) indicated that the relationship between Behavioural Intention and Perceived vulnerability is partially mediated by Perceived severity. The results showed that Perceived severity is partially mediating the relationship between Behavioural Intention and Perceived vulnerability as the indirect effects were statistically significant ($\beta = 0.02$, $p < 0.001$). The coefficient ($\beta = 0.02$)

indicates the strength of the indirect effect of Behavioural Intention on Perceived vulnerability through Perceived severity. A positive coefficient suggests that there is a positive relationship between the variables (i.e., as Behavioural Intention increases, so does Perceived vulnerability through Perceived severity). The *p*-value ($p < 0.001$) indicates the level of statistical significance of the mediation effect. A *p*-value less than 0.05 suggests that the mediation effect is statistically significant, meaning that the indirect effect is unlikely to have occurred by chance.

In summary, the results of the mediation test suggest that Perceived severity partially mediates the relationship between Behavioural Intention and Perceived vulnerability, meaning that the perceived severity of the problem or issue is influencing the extent to which an individual perceives themselves as vulnerable, and this effect is statistically significant.

There is an absence of identified information security studies that measured the mediation effect of Perceived severity on Perceived vulnerability and Behavioural Intention in the context of practising information security or good cybersecurity behaviours. This gap highlights the need for more research on this finding, however by examining and establishing this relationship, this study contributed to addressing the existing knowledge gap. By investigating this mediation relationship, this study provides empirical evidence for the relationship, which contributes to a broader understanding of the psychological and cognitive factors that shape individuals' attitudes and behaviours regarding practising good cybersecurity behaviours. This finding identifies a factor that enhances an individual's Perceived vulnerability and subsequently influences their intention to practise good cybersecurity behaviours. This knowledge can help inform future development of targeted interventions, education programmes and awareness campaigns to promote better cybersecurity practices.

The sixth hypothesis of this study explored the impact of Self-efficacy on an individual's behavioural intention to practice good cybersecurity behaviours. The results showed (see Table 4-10 in section 4.4.3) a positive but not very significant effect ($\beta = 0.08$, $t = 1.30$, $p = 0.19$), which led to H6 not being supported. Self-efficacy refers to an individual's belief in their capacity and resources to carry out a specific behaviour (Pham et al., 2017). This finding contradicts previous research that found Self-efficacy to have a significant positive influence on behavioural intention, such as the studies conducted by Johnston & Warkentin (2010), Crossler & Bélanger (2014), and Zhang et al. (2009). However, similar results were found in previous research by Kim, Yang & Park (2014) and Hovav & Putri (2016). To further understand why Self-efficacy may improve behavioural intention in some cases and not others, additional research is needed. This could involve exploring other factors that may moderate the relationship between Self-efficacy and behavioural intention or investigating how Self-efficacy is perceived and measured in different contexts.

The seventh hypothesis aimed to examine the relationship between Response efficacy and an individual's Behavioural Intention to practice good cybersecurity behaviours. The findings (see Table 4-10 in section 4.4.3) indicate that there is a positive and significant effect of Response efficacy on Behavioural Intention, which supports H7 ($\beta = 0.13$, $t = 2.27$, $p = 0.02$). Response efficacy refers to the belief that taking the recommended action will help in mitigating the threat event. The results of the study suggest that an individual's belief in the effectiveness of their actions can influence their intention to adopt good cybersecurity practices. This is consistent with the PMT and is supported by previous studies in the IS domain (Crossler & Bélanger, 2014; Hanus & Wu, 2016; Hovav & Putri, 2016; Ifinedo, 2012; Johnston & Warkentin, 2010; Kim et al., 2014; Yoon et al., 2012). The findings suggest that it is important to educate individuals on the effectiveness of good cybersecurity behaviours to increase their response efficacy beliefs. This can help in promoting positive intentions towards practising good cybersecurity behaviours.

The eighth hypothesis of this study examined whether Response Costs associated with good cybersecurity behaviours have a negative effect on an individual’s behavioural intention to practise good cybersecurity behaviours. The analysis showed (see Table 4-10 in section 4.4.3) that the effect of Response Cost on Behavioural Intention was negative but not significant ($\beta = -0.03$, $t = -0.55$, $p = 0.58$). Response costs refer to any monetary, non-monetary barriers that might be experienced when practising good cybersecurity behaviour. The results indicate that Response cost negatively influences an individual’s intention to practice good cybersecurity behaviours, but the effect is not significant, hence H8 was not supported. This does not support the original PMT theory, but similar results have been found in previous studies like Ifinedo (2012) and Hanus & Wu (2016). Ifinedo's (2012) study in an organisational context found similar results to this study. The results of their study showed that Response cost does have a negative effect on compliance intention but the strength of the relationship was not significant (Ifinedo, 2012). Alternatively, the study by Hanus & Wu (2016), which investigated desktop security behaviour of home users found the effect of Response costs to be insignificant. The authors posited that the insignificant effect of Response cost could be due to the high availability and affordability of software countermeasures like antivirus (Hanus & Wu, 2016).

The ninth hypothesis in this study was related to the differences in education levels and the factors that influence an individual's intention to practise good cybersecurity behaviours. The different groups of levels of education are Matric, Undergraduate (Diploma), Undergraduate (Bachelor's degree), Postgraduate (Honours degree), Postgraduate (Master's degree), Postgraduate (PhD degree) and Other (mostly certificates). The analysis revealed that there were no differences across the education level groups and an individual's behavioural intention to practise good cybersecurity behaviours. Thus, the ninth hypothesis is rejected. This result contradicts a similar study on information security awareness by Öğütçü, Testik and Chouseinoglou (2016). In their research, they found that higher education levels resulted in more information security awareness (Öğütçü, Testik & Chouseinoglou, 2016). A study by Fatokun, Hamid, Norman & Fatokun (2019) found that, though education level had some impact on good cybersecurity behaviours, the impact was minute compared to age and gender of respondents. The authors posit that this nearly insignificant impact could suggest that education level may not necessarily effect an individual's good cybersecurity behaviours (Fatokun, Hamid, Norman & Fatokun, 2019).

The tenth and final hypothesis for this study posited that there would be significant differences between the levels of time spent on the Internet and the factors that influence an individual's behavioural intention to practise good cybersecurity behaviours. The different group levels are Less than two hours per day, 2-4 hours per day, 5-8 hours per day, and more than 8 hours per day. The results of the analysis revealed differences across the levels of time spent on the Internet and the factors of

Attitude towards good cybersecurity behaviour, Behavioural Intention and Subjective norms. This suggests that the amount of time spent on the Internet had a significant effect on an individual's Attitude towards good cybersecurity behaviours, Subjective norms, and Behavioural Intention. Thus, the tenth hypothesis is accepted. The finding of this study that Internet usage has a significant effect on an individual’s cybersecurity behaviours is similar to findings from previous studies.

A study by Zwilling et al. (2020) found that there was a relationship between Internet usage and cybersecurity behaviours, through the mediation variable of cybersecurity awareness. The authors posit that, though usage is a factor in performing good cybersecurity behaviours, it is the level of awareness that has the most significant effect (Zwilling et al., 2020). Another study by Duman (2022) found that students’ cybersecurity behaviours do differ according to daily Internet usage levels. The authors found that students with lower daily Internet usage levels have higher cyber security awareness levels (Duman, 2022).

5.3 Implications for theory and practise

5.3.1 Theoretical implications

This study made use of a combination of two theoretical frameworks which formed the basis of this study. The TPB was developed by Ajzen (1991) and the PMT was developed by Rogers (1975) and revised by Maddux & Rogers (Maddux & Rogers, 1983). The TPB endeavours to predict human behaviour (Ajzen, 1991), while the PMT aims to explore the factor of fear appeals influencing attitude and behaviour (Broer & Seydel, 1996). The findings of this study supported two of the three constructs from TPB as significant influencers of behavioural intention in individuals (Attitude towards good cybersecurity behaviour and Subjective norm). However, the Self-efficacy construct of TPB was not supported by the findings in this study. To further understand why Self-efficacy may improve Behavioural Intention in some cases and not others, additional research is needed. This could involve exploring other factors that may moderate the relationship between Self-efficacy and Behavioural Intention or investigating how Self-efficacy is perceived and measured in different contexts.

The findings of this study supported two of the five constructs of PMT as significant influencers of an individual’s behavioural intention, mainly Perceived severity and Response efficacy. The findings of this study did not support the influence of Perceived vulnerability, Self-efficacy, and Response cost on an individual’s intention to practice good cybersecurity behaviours.

The findings of this study identified a mediation relationship between Perceived vulnerability and Behavioural Intention through Perceived severity. This mediation relationship is not hypothesised in the original PMT model; therefore, the identification of the mediation relationship could potentially enrich the original PMT theory. The dearth of studies quantifying the mediation effect of Perceived severity on Perceived vulnerability and Behavioural Intention in the context of information security points to the necessity of further study in this field. This research extends the theoretical landscape of information security studies and offers insights into the underlying mechanisms influencing people's decision-making processes by employing mediation analysis in this particular setting. This finding identifies a factor that enhances an individual’s Perceived vulnerability and subsequently influences their intention to practise good cybersecurity behaviours. This knowledge can help inform future development of targeted interventions, education programmes and awareness campaigns to promote better cybersecurity practices.

5.3.2 Practical implications

This study contributes to the existing research on information security and good cybersecurity behaviours and the factors that influence them. This study mainly contributes to the cybersecurity body of knowledge, specifically focusing on South Africans. Many international studies researched the factors influencing good cybersecurity behaviours, but the results are varied and range from country to country (Crossler & Bélanger, 2014; Yoon & Kim, 2013). There seems to be limited research into the wide range of factors that might influence and impact South Africans practising good cybersecurity behaviours while online. Most of the research conducted in South Africa focuses on awareness and implementation of awareness in the country (de Bruijn & Janssen, 2017; Gcaza & von Solms, 2017; Grobler et al., 2011). Therefore, this study focusing on influencers of South African's good cybersecurity behavioural intention is crucial.

The audiences that might benefit from this study include South African citizens, academics, policymakers, government regulators and organisations in South Africa. Academics, regulators, organisations, and the Government will benefit from this study by gaining more insight into the factors that influence South Africans to practise good cybersecurity behaviours, which can be used in their future cybersecurity strategies. This knowledge can help inform future development of targeted interventions, education programmes and awareness campaigns to promote better cybersecurity practices. This information could potentially be utilised in the future as the basis for other researchers' studies.

5.3.3 Limitations

One limitation of the study is that it only focused on South African participants, which may limit the generalisability of the findings to other populations with different cultures, backgrounds, and contexts. Therefore, it is crucial to consider the potential cultural and regional factors that could influence the participants' good cybersecurity behaviours.

Another limitation of the study is that the data collected relied on self-reported measures, which may be subject to social desirability bias, leading participants to over-report their cybersecurity behaviours. Thus, future research could use additional methods to measure behavioural intention, such as direct observation or behavioural logs.

Furthermore, as cybersecurity is a complex and multifaceted issue, the study's quantitative nature may have overlooked some important nuances in the participants' experiences and behaviours. A qualitative approach could help gain a deeper understanding of the subjective experiences and motivations that drive good cybersecurity behaviour. Additionally, a qualitative research approach could explore the individual, social, and cultural factors that influence users' good cybersecurity behaviours.

5.3.4 Future research

There is a need for further research on Self-efficacy and its impact on good cybersecurity behaviour. It may be beneficial to explore additional factors that may moderate or mediate this relationship. For example, factors such as age, gender, and education level may influence how Self-efficacy impacts behavioural intention. It may be useful to examine how situational factors, such as the type of cyberthreat or the context in which the behaviour occurs, may impact this relationship.

Future research could include measuring actual behaviour instead of self-reported Behavioural Intention. This approach could provide a more accurate picture of the cybersecurity behaviours of South Africans. A study using this approach could explore the factors that influence actual behaviour, such as perceived control, and the availability of resources.

Furthermore, investigating cybersecurity behaviour on mobile devices in South Africa could be a valuable extension of this study. As mobile devices are becoming more prevalent and are often used to access sensitive personal information, understanding the cybersecurity behaviours of South Africans on these devices could provide insights into the vulnerabilities of these devices and how to address them. The study by Giwah, Wang, Levy & Hur (2020) provides a useful framework for investigating this topic and could be adapted for use in a South African context.

5.4 Conclusion

This study aimed to discover what factors had the most influence on a South African’s behavioural intention to practise good cybersecurity behaviours. This study was able to show Attitudes towards good cybersecurity behaviours, Subjective norms, Perceived severity, and Response efficacy have the most significant effect on an individual’s intention to practice good cybersecurity behaviours. This means that to increase the practice of good cybersecurity behaviours amongst South Africans, there needs to be a focus on how to influence these factors in individuals. Cybersecurity awareness and training programmes are used to share knowledge on cybersecurity risks and encourage practising good cybersecurity behaviour (Gundu, 2019; Kritzinger et al., 2017). Using awareness campaigns or training to target and change the attitude towards good cybersecurity behaviours in South Africa has the potential to influence cybersecurity behaviour in the county. Subjective norms could be targeted similarly, through awareness campaigns and training.

Due to the adverse effects of cyberattacks and cyberthreats on the individual, it becomes vital to understand the cybersecurity behaviours and processes individuals follow and to pinpoint the determinants of these behaviours (Bulgurcu et al., 2010; Crossler & Bélanger, 2014). Perceived severity was found to have a significant effect on behavioural intention. Targeted cyberthreat severity campaigns could be used to increase the understanding of the severity of cyberthreats, which could have a significant impact on South Africans practising good cybersecurity behaviours. Response efficacy was found to be a significant influencer of behavioural intention. This means that South Africans do believe that practising good cybersecurity behaviours will result in a positive outcome of not being a victim of a cyberthreat.

Overall, this study highlights the importance of understanding the factors that influence individuals' intentions to practice good cybersecurity behaviours. By targeting and changing Attitudes, Subjective norms, Perceived severity, and Response efficacy, it might be possible to increase the practice of good cybersecurity behaviours in South Africans and mitigate the risks associated with cyberthreats.

List of references

Ab Hamid, M. R., Samil, W., & Sidek, M. H. (2017). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion *Journal of Physics: Conference Series*,890. Pahang, Malaysia.8-10 August 2017.[Online] Retrieved from: https://iopscience.iop.org/article/10.1088/1742-6596/890/1/012163/meta [Accessed: 2023-03-11]

Aderibigbe, N., & Ocholla, D. N. (2020). Insight into ethical cyber behaviour of undergraduate students at selected African universities. *SA Journal of Information Management*, *22*, 8. Retrieved from: https://doi.org/10.4102/sajim.v22i1.1131 [Accessed: 2022-04-15]

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2020). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 1-20. Retrieved from: https://doi.org/10.1080/0144929X.2020.1856928 [Accessed: 2022-04-14]

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211. Retrieved from: https://doi.org/10.1016/0749-5978(91)90020-T [Accessed: 2021-02-02]

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Applied Sciences*, *13*(9), 5700. Retrieved from: https://doi.org/10.3390/app13095700 [Accessed: 2022-05-15]

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613-643. Retrieved from: https://doi.org/10.2307/25750694 [Accessed: 2021/02/22]

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411-423. Retrieved from: https://doi.org/10.1037/0033-2909.103.3.411 [Accessed: 2022-03-15]

Aurigemma, S. (2013). A Composite Framework for Behavioral Compliance with Information Security Policies. *Journal of Organizational and End User Computing*, *25*(3), 67-82. Retrieved from: https://doi.org/10.4018/joeuc.2013070103 [Accessed: 2022-05-15]

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74-94. Retrieved from: https://doi.org/10.1007/BF02723327 [Accessed: 2023-02-15]

Baron, R., & Kenny, D. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*, 1173-1182. Retrieved from: https://doi.org/10.1037//0022-3514.51.6.1173 [Accessed: 2023-02-24]

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin*, *107*(2), 238-246. Retrieved from: https://doi.org/10.1037/0033-2909.107.2.238 [Accessed: 2023-03-01]

Bhana, A. (2020). *Should I download the new contact tracing app?* Retrieved from:https://www.explain.co.za/2020/09/15/explainer-should-i-download-the-new-contact-tracing-app/ [Accessed: 2020-02-21]

Boone, H. N., & Boone, D. A. (2012). Analyzing likert data. *Journal of extension*, *50*(2), 1-5. Retrieved from: https://tigerprints.clemson.edu/joe/vol50/iss2/48 [Accessed: 2023-03-01]

Botes, M. (2020). *Unpacking the legal and ethical aspects of South Africa's COVID-19 track and trace app*. Retrieved from:https://theconversation.com/unpacking-the-legal-and-ethical-aspects-of-south-africas-covid-19-track-and-trace-app-147137 [Accessed: 2021-02-21]

Braun, N. K. H. (2014). *An Exploration of the Factors Influencing Home Users' Cybersecurity Behaviours* Victoria University of Wellington. Victoria University of Wellington http://hdl.handle.net/10063/3244

Broer, H., & Seydel, E. R. (1996). Protection Motivation Theory. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour: Research and Practice with Social Cognition Models. Eds. Mark Conner, Paul Norman*. Open University Press.

Brown, T. A. (2006). *Confirmatory factor analysis for applied research*.New York, NY, US: The Guilford Press. [Online] Retrieved from:http://www.kharazmi-statistics.ir/Uploads/Public/book/Methodology%20in%20the%20Social%20Sciences.pdf [Accessed: 2023-02-14]

Browne, M. W., & Cudeck, R. (1992). Alternative Ways of Assessing Model Fit. *Sociological Methods & Research*, *21*(2), 230-258. Retrieved from: https://doi.org/10.1177/0049124192021002005 [Accessed: 2023-03-01]

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548. Retrieved from: https://doi.org/10.2307/25750690 [Accessed: 2022-05-02]

BusinessTech. (2021). *What South Africans should know about the changes to WhatsApp: legal expert*. Retrieved from:https://businesstech.co.za/news/technology/460204/what-south-africans-should-know-about-the-changes-to-whatsapp-legal-expert/ [Accessed: 21 February 2021]

Byrne, B. M. (2010). *Structural Equation Modeling With AMOS: Basic Concepts, Applications, and Programming, Second Edition* (2nd ed.).New York: Routledge. [Online] Retrieved from:https://www.researchgate.net/file.PostFileLoader.html?id=551bcf4cd2fd6

424088b45e4&assetKey=AS:273770781052931@1442283449007 [Accessed: 2023-02-14]

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36-45. Retrieved from: https://doi.org/10.1016/j.jisa.2018.08.002 [Accessed: 2022-05-02]

Carugati, A., Mola, L., Plé, L., Lauwers, M., & Giangreco, A. (2020). Exploitation and exploration of IT in times of pandemic: from dealing with emergency to institutionalising crisis practices. *European Journal of Information Systems*, *29*(6), 762-777. Retrieved from: https://doi.org/10.1080/0960085X.2020.1832868 [Accessed: 2022-07-06]

Chen, T., Xu, M., Tu, J., Wang, H., & Niu, X. (2018). Relationship between Omnibus and Post-hoc Tests: An Investigation of performance of the F test in ANOVA. *Shanghai Arch Psychiatry*, *30*(1), 60-64. Retrieved from: https://doi.org/10.11919/j.issn.1002-0829.218014 [Accessed: 2023-02-05]

Chen, Y., & Zahedi, F. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*, *40*(1), 205-222. Retrieved from: https://doi.org/10.25300/MISQ/2016/40.1.09 [Accessed: 2022-07-06]

Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment*, *7*(3), 309-319. Retrieved from: https://doi.org/10.1037/1040-3590.7.3.309 [Accessed: 2023-02-01]

Collier, J. E. (2020). *Applied structural equation modeling using AMOS : basic to advanced techniques*.London, UK: Routledge. [Online] Retrieved from:https://www.researchgate.net/publication/341667182_Applied_Structural_Equation_Modeling_Using_AMOS_Basic_to_Advanced_Techniques [Accessed: 2023-03-04]

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *ACM SIGMIS Database*, *45*(4), 51-71. Retrieved from: https://doi.org/10.1145/2691517.2691521 [Accessed: 2022-05-02]

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101. Retrieved from: https://doi.org/10.1016/j.cose.2012.09.010 [Accessed: 2022-05-02]

Cybersecurity Hub. (2019). *About Us*. [Online] Retrieved from: https://www.cybersecurityhub.gov.za/about-us [Accessed: 1 March]

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. Retrieved from: https://doi.org/10.1016/j.giq.2017.02.007 [Accessed: 2022-05-02]

DeCoster, J., & Claypool, H. M. (2004). *Data Analysis in SPSS*. Retrieved from:http://www.stat-help.com/notes.html [Accessed: 2023-01-23]

Denis, D. J. (2020). *Univariate, bivariate, and multivariate statistics using R : quantitative tools for data analysis and data science*.Hoboken, NJ: Wiley. [Online] Retrieved from:https://doi.org/10.1002/9781119549963 [Accessed: 2023-03-24]

DeVellis, R. F. (2012). *Scale development : theory and applications* (3rd ed.).New York: Sage Publications. [Online] Retrieved from:https://www.academia.edu/42875983/Scale_Developm_ent_Theory_and_Applications_Second_Edition [Accessed: 2023-02-24]

Dhir, A., Yossatorn, Y., Kaur, P., & Chen, S. (2018). Online social media fatigue and psychological wellbeing—A study of compulsive use, fear of missing out, fatigue, anxiety and depression. *International Journal of Information*

Management, *40*, 141-152. Retrieved from: https://doi.org/10.1016/j.ijinfomgt.2018.01.012 [Accessed: 2022-05-26]

Dill, K. J. (2018). Cybersecurity for the Nation Workforce Development. *The Cyber Defense Review*, *3*(2), 55-64. Retrieved from: www.jstor.org/stable/26491223 [Accessed: 2020/02/28]

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386-392,394-408. Retrieved from: https://doi.org/10.17705/1jais.00133 [Accessed: 2022-05-26]

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*, 102056. Retrieved from: https://doi.org/10.1016/j.ijinfomgt.2019.102056 [Accessed: 2022-04-24]

Duman, F. K. (2022). Determining Cyber Security-Related Behaviors of Internet Users: Example of the Faculty of Sport Sciences Students. *European Journal of Education*, *5*(1), 112-128. Retrieved from: https://doi.org/10.26417/723gru15 [Accessed: 2023-02-14]

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N. P., Sharma, S. K., & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, *55*, 102211. Retrieved from: https://doi.org/10.1016/j.ijinfomgt.2020.102211 [Accessed: 2022-05-26]

Evans, M., Maglaras, L., He, Y., & Janicke, H. (2016). Human Behaviour as an aspect of Cyber Security Assurance. *Security and Communication Networks*, *9*. Retrieved from: https://doi.org/10.1002/sec.1657 [Accessed: 2022-05-26]

Fabrigar, L., Wegener, D., MacCallum, R., & Strahan, E. (1999). Evaluating the Use of Exploratory Factor Analysis in Psychological Research. *Psychological Methods*, *4*(3), 272. Retrieved from: https://doi.org/10.1037/1082-989X.4.3.272 [Accessed: 2022-05-26]

Farooq, A., Ndiege, J., & Isoaho, J. (2019). Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior. Retrieved from: https://doi.org/10.1109/AFRICON46755.2019.9133764 [Accessed: 2022-04-01]

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, *1339*(1), 012098. Retrieved from: https://doi.org/10.1088/1742-6596/1339/1/012098 [Accessed: 2022-05-26]

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*.London, UK: Sage Publications Ltd. [Online] Retrieved from:https://www.researchgate.net/profile/Abdelrahman_Zueter2/post/What_are_the_conditions_for_using_Ordinal_Logistic_regression_Can_anyone_share_the_various_regression_methods_and_their_application/attachment/59d637d8c49f478072ea5080/AS:273691429015552@1442264529487/download/DISCOVERING+STATISTICS.pdf [Accessed: 2023-02-26]

Foltz, C. B., Newkirk, H. E., & Schwager, P. H. (2016). An Empirical Investigation of Factors that Influence Individual Behavior toward Changing Social Networking Security Settings. *Journal of Theoretical and Applied Electronic Commerce Research*, *11*(2), 1-15. Retrieved from: https://doi.org/10.4067/S0718-18762016000200002 [Accessed: 2022-08-14]

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing*

Research, *18*(1), 39-50. Retrieved from: https://doi.org/10.2307/3151312 [Accessed: 2023-02-26]

French, A., Macedo, M., Poulsen, J., Waterson, T., & Yu, A. (2008). Multivariate analysis of variance (MANOVA). Retrieved from: https://www.coursehero.com/file/8673766/MANOVAnewest/ [Accessed: 2023-02-26]

Fricker, R. D. (2008). The SAGE Handbook of Online Research Methods. In (pp. 195-216). SAGE Publications, Ltd.[Online] Retrieved from:https://methods.sagepub.com/book/the-sage-handbook-of-online-research-methods [Accessed: 2023-02-26]

Gcaza, N., & von Solms, R. (2017). A Strategy for a Cybersecurity Culture: A South African Perspective. *The Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1-17. Retrieved from: https://doi.org/10.1002/j.1681-4835.2017.tb00590.x [Accessed: 2022-02-26]

Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2020). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory [Article]. *Journal of Intellectual Capital*, *21*(2), 215-233. Retrieved from: https://doi.org/10.1108/JIC-03-2019-0063 [Accessed: 2022-05-16]

Government Gazette. (2013). *Protection of Personal Information Act*. Retrieved from:https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Grimes, M., & Marquardson, J. (2019). Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, *119*, 23-34. Retrieved from: https://doi.org/10.1016/j.dss.2019.02.010 [Accessed: 2022-04-01]

Grobler, M., Dlamini, Z., Ngobeni, S., & Labuschagne, W. A. (2011). Towards a Cyber security aware rural community *2011 Information Security for South Africa (ISSA) Conference*,Hayatt Regency Hotel, Rosebank, Johannesburg, South Africa.[Online] Retrieved from: http://hdl.handle.net/10204/5183 [Accessed: 2022-02-26]

Grobler, M., Jansen van Vuuren, J., & Leenen, L. (2012). Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward *10th IFIP TC9 International Conference on Human Choice and Computers*,386. Amsterdam, Netherlands.[Online] Retrieved from: https://link.springer.com/chapter/10.1007/978-3-642-33332-3_20#citeas [Accessed: 2023-02-26]

Grobler, M., Jansen van Vuuren, J. C., & Zaaiman, J. (2013). Evaluating cyber security awareness in South Africa *10th European Conference on Information Warfare and Security*,Estonia.7-8 July 2011.[Online] Retrieved from: http://hdl.handle.net/10204/5108 [Accessed: 2022-07-26]

Gundu, T. (2019). Big Data Big Security and Privacy Risks: Bridging Employee Knowledge and Actions Gap. *Journal of Information Warfare*, *18*(2), 15-30. Retrieved from: https://www.jstor.org/stable/26894668 [Accessed: 2023-02-26]

Hahs-Vaughn, D. L. (2016). *Applied multivariate statistical concepts* (1st edition ed.).New York, US: Routledge. [Online] Retrieved from:https://www.taylorfrancis.com/books/mono/10.4324/9781315816685/applied-multivariate-statistical-concepts-debbie-hahs-vaughn [Accessed: 2023-02-26]

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate Data Analysis: A Global Perspective* (7th Edition ed.).Upper Saddle River, NJ: Pearson Education. [Online] Retrieved from:https://www.drnishikantjha.com/papersCollection/Multivariate%20Data%20Analysis.pdf [Accessed: 2023-02-26]

Hair, J., Ringle, C., & Sarstedt, M. (2013). Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance. *Long Range Planning*, *46*(6), 1-12. Retrieved from: https://doi.org/10.1016/j.lrp.2013.08.016 [Accessed: 2023-03-11]

Hanus, B., & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2-16. Retrieved from: https://doi.org/10.1080/10580530.2015.1117842 [Accessed: 2023-03-11]

Hassandoust, F., Techatassanasoontorn, A. A., & Singh, H. (2020). *Information Security Behaviour: A Critical Review and Research Directions*. An Online AIS Conference. In Proceedings of the 28th European Conference on Information Systems (ECIS). 15-17 June 2020.[Online] Retrieved from: https://aisel.aisnet.org/ecis2020_rp/71/ [Accessed: 2023-03-11]

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*, 115-135. Retrieved from: https://doi.org/10.1007/s11747-014-0403-8 [Accessed: 2023-03-11]

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35-49. Retrieved from: https://doi.org/doi.org/10.1016/j.pmcj.2016.06.007 [Accessed: 2022-07-16]

Hu, L.-t., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological Methods*, *3*(4), 424-453. Retrieved from: https://doi.org/10.1037/1082-989X.3.4.424 [Accessed: 2023-03-11]

IBM Security. (2022). *Cost of a Data Breach Report 2022*. [Online] Retrieved from: https://www.ibm.com/reports/data-breach [Accessed: 2023-05-05]

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. *Policy Design and Practice*, *6*(2), 146-159. Retrieved from: https://doi.org/10.1080/25741292.2023.2199960

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. Retrieved from: https://doi.org/10.1016/j.cose.2011.10.007 [Accessed: 2022-03-11]

Information Regulator South Africa. (2021). *The Information Regulator is assessing the compliance of the revised WhatsApp Privacy Policy*. Press statement issued on: 13 January 2021. [Online] Retrieved from: https://inforegulator.org.za/wp-content/uploads/2020/07/ms-20210113-Whatsapp.pdf [Accessed: 2021-02-21]

Interpol. (2023). *African cyberthreat assessment report cyberthreat trends*. [Online] Retrieved from: https://www.interpol.int/content/download/19174/file/2023_03%20CYBER_African%20Cyberthreat%20Assessment%20Report%202022_EN.pdf [Accessed: 16 October 2023]

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research*, *22*(1). Retrieved from: https://doi.org/10.2196/16775 [Accessed: 2022-03-11]

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40-55. Retrieved from: https://doi.org/10.1016/j.ijhcs.2018.10.004 [Accessed: 2022-03-11]

Jere, J. N. (2020). Investigating university academics behavioural intention in the adoption of e-learning in a time of COVID-19. *South African Journal of*

Information Management, *22*(1), 1-9. Retrieved from: https://doi.org/10.4102/sajim.v22i1.1280 [Accessed: 2023-03-11]

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549-566. Retrieved from: https://doi.org/10.2307/25750691 [Accessed: 2023-03-11]

Kemp, S. (2023). *Digital 2023: South Africa*. [Online] Retrieved from: https://datareportal.com/reports/digital-2023-south-africa [Accessed: 2023-05-25]

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *ScientificWorldJournal*, *2014*, 463870. Retrieved from: https://doi.org/10.1155/2014/463870 [Accessed: 2022-06-04]

Klaaren, J., Breckenridge, K., Cachalia, F., Fonn, S., & Veller, M. (2020). South Africa’s COVID-19 Tracing Database: Risks and rewards of which doctors should be aware [Contact tracing; Informational privacy; COVID-19 pandemic]. *South African Medical Journal*, *110*(7). Retrieved from: http://www.samj.org.za/index.php/samj/article/view/12983/9381 [Accessed: 2022-03-11]

Kline, R., & St, C. (2022). *Principles and Practice of Structural Equation Modeling*.New York, US: The Guilford Press. [Online] Retrieved from:https://www.researchgate.net/profile/Cahyono-St/publication/361910413_Principles_and_Practice_of_Structural_Equation_Modeling/links/62cc4f0ed7bd92231faa4db1/Principles-and-Practice-of-Structural-Equation-Modeling.pdf [Accessed: 2023-03-11]

Kritzinger, E., Bada, M., & Nurse, J. (2017). A Study into the Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK *IFIP World Conference on Information Security Education*,503. [Online] Retrieved from: https://link.springer.com/chapter/10.1007/978-3-319-58553-6_10 [Accessed: 2022-03-11]

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77-81. Retrieved from: https://doi.org/10.1080/1097198X.2019.1603527 [Accessed: 2023-03-11]

Kwak, S., & Kim, J. (2017). Central limit theorem: The cornerstone of modern statistics. *Korean Journal of Anesthesiology*, *70*(2), 144. Retrieved from: https://doi.org/10.4097/kjae.2017.70.2.144 [Accessed: 2022-04-11]

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469-479. Retrieved from: https://doi.org/10.1016/0022-1031(83)90023-9 [Accessed: 2021-03-11]

Marsh, H. W., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First- and higher order factor models and their invariance across groups. *Psychological Bulletin*, *97*(3), 562-582. Retrieved from: https://doi.org/10.1037/0033-2909.97.3.562 [Accessed: 2023-03-11]

McRobert, C. J., Hill, J. C., Smale, T., Hay, E. M., & van der Windt, D. A. (2018). A multi-modal recruitment strategy using social media and internet-mediated methods to recruit a multidisciplinary, international sample of clinicians to an online research study. *PLoS ONE*, *13*(7). Retrieved from: https://doi.org/10.1371/journal.pone.0200184 [Accessed: 2022-03-11]

Michalsons. (2022). *Protection of Personal Information Act Summary | POPIA*. [Online] Retrieved from: https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia [Accessed: 2023-03-11]

Mills, A., & Sahi, N. (2019). *An empirical study of home user intentions towards computer security*. Proceedings of the 52nd Hawaii International Conference on System Sciences. [Online] Retrieved from: http://hdl.handle.net/10125/59921 [Accessed: 2022-07-18]

Mitrovic, Z. (2018). *Who will protect our digital future, Mr President?* [Online] Retrieved from: https://www.news24.com/MyNews24/who-will-protect-our-digital-future-mr-president-20180928 [Accessed: 2022-07-18]

Mitrovic, Z., Colab, K., Thakur, S., & Phukubje, P. (2019). Towards a Model for Building Public Awareness for Successful Cybersecurity Skilling *Digital innovation and transformation conference*,Gauteng, South Africa.[Online] Retrieved from: https://www.researchgate.net/publication/335453265_TOWARDS_A_MODEL_FOR_BUILDING_PUBLIC_AWARENESS_FOR_SUCCESSFUL_CYBERSECURITY_SKILLING [Accessed: 2022-07-18]

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*. Retrieved from: https://doi.org/10.3389/fpsyg.2021.561011 [Accessed: 2022-07-19]

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

Mtuze, S. S. K., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*. Retrieved from: https://doi.org/10.1365/s43439-023-00089-8 [Accessed: 2023-06-30]

MyBroadband. (2021). *WhatsApp privacy concerns in South Africa explained*. Retrieved from:https://mybroadband.co.za/news/security/384886-whatsapp-privacy-concerns-in-south-africa-explained.html#:~:text=South%20Africa's%20privacy%20laws%20are,they%20further%20process%20this%20data. [Accessed: 2021-02-21]

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306-321. Retrieved from: https://doi.org/10.1080/0960085X.2020.1771222 [Accessed: 2022-03-25]

Nedbank. (2020). *Nedbank warns clients of potential impact of data incident at Computer Facilities (Pty) Ltd*. [Online] Retrieved from: https://www.nedbank.co.za/content/nedbank/desktop/gt/en/info/campaigns/nedbank-warns-clients.html [Accessed: 2021-02-21]

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.).New York, US: McGraw-Hill. [Online] Retrieved from:https://doi.org/10.1177/073428299901700307 [Accessed: 2022-07-18]

Oates, B. J. (2006). *Researching Information Systems and Computing*.California, US: Sage Publications Ltd. [Online] Retrieved from:http://uk.sagepub.com/sites/default/files/upm-binaries/9811_037126intro.pdf [Accessed: 2022-01-18]

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93. Retrieved from: https://doi.org/10.1016/j.cose.2015.10.002 [Accessed: 2022-07-18]

Pallant, J. (2011). *Spss survival manual : a step by step guide to data analysis using spss* (4th ed.).London, UK: Routledge. [Online] Retrieved from:https://lms.su.edu.pk/download?filename=1588697869-julie-pallant-spss-survival-manual-mcgraw-hill-house-2016-1.pdf&lesson=17247 [Accessed: 2023-02-06]

Peter, A. S. (2017). Cyber resilience preparedness of Africa’s top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, *17*, 49-59. Retrieved from:

Peters, A., & Jordan, A. (2019). *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*. [Online] Retrieved from: www.jstor.org/stable/resrep20150 [Accessed: 2020-02-08]

Pham, H.-C., Brennan, L., & Richardson, J. (2017). *Review of behavioural theories in security compliance and research challenge*. Proceedings of the Informing Science and Information Technology Education Conference. Vietnam,pp. 65-76.Santa Rosa, CA: Informing Science Institute. [Online] Retrieved from: http://www.informingscience.org/Publications/3722 [Accessed: 2023-02-06]

Pieterse, H. (2021). The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication*, *28*, 1-21. Retrieved from: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2077-72132021000200003&nrm=iso [Accessed: 2023-05-06]

Pituch, K. A., & Stevens, J. P. (2012). *Applied multivariate statistics for the social sciences* (6th ed.).London, UK: Routledge. [Online] Retrieved from:https://digilibadmin.unismuh.ac.id/upload/26551-Full_Text.pdf [Accessed: 2023-05-01]

PricewaterhouseCoopers. (2020). *PwC's Global Economic Crime and Fraud Survey*. [Online] Retrieved from: https://www.pwc.co.za/en/assets/pdf/global-economic-crime-survey-2020.pdf [Accessed: 2023-05-06]

Retutas, M., & Rubio, M. (2021). Multivariate analysis on performance in statistics, self-efficacy and attitudes of senior high school students. *JRAMathEdu (Journal of Research and Advances in Mathematics Education)*, *6*(4), 352-367. Retrieved from: https://doi.org/10.23917/jramathedu.v6i4.14368 [Accessed: 2023-02-06]

Richardson, J. T. E. (2011). Eta squared and partial eta squared as measures of effect size in educational research. *Educational Research Review*, *6*(2), 135-

147. Retrieved from: https://doi.org/10.1016/j.edurev.2010.12.001 [Accessed: 2023-02-06]

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93-114. Retrieved from: https://doi.org/10.1080/00223980.1975.9915803 [Accessed: 2022-05-01]

Ruxton, G. D., & Beauchamp, G. (2008). Time for some a priori thinking about post hoc testing. *Behavioral Ecology*, *19*(3), 690-693. Retrieved from: https://doi.org/10.1093/beheco/arn020 [Accessed: 2023-04-06]

Schumacker, R. E., & Lomax, R. G. (2004). *A beginner's guide to structural equation modeling* (2nd ed.).Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers. [Online] Retrieved from:https://www.taylorfrancis.com/books/mono/10.4324/9781410610904/beginner-guide-structural-equation-modeling-randall-schumacker-richard-lomax [Accessed: 2023-02-06]

Shapshak, T. (2019). *South Africa Has Second Most Android Banking Malware Attacks As Cyber Crime Increases*. [Online] Retrieved from: https://www.forbes.com/sites/tobyshapshak/2019/05/09/south-africa-has-second-most-android-banking-malware-attacks-as-cyber-crime-increases/#3a8eb51a5d77 [Accessed: 2022-02-06]

Shrestha, N. (2021). Factor Analysis as a Tool for Survey Analysis. *American Journal of Applied Mathematics and Statistics*, *9*(1), 4-11. Retrieved from: https://doi.org/10.12691/ajams-9-1-2 [Accessed: 2023-02-06]

Silva, D. L., Sabino, L. D., Lanuza, D. M., Adina, E. M., Villaverde, B. S., & Pena, E. G. (2014). *Silva’s management competency theory: a factor-item analytic approach utilizing oblique rotation direct oblimin method under kaiser-bartlett’s test of sphericity* https://www.iaeng.org/publication/WCECS2014/WCECS2014_pp300-305.pdf

Siponen, M., Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2). Retrieved from: https://doi.org/10.1016/j.im.2013.08.006 [Accessed: 2023-02-06]

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, *43*(2), 64-71. Retrieved from: https://doi.org/10.1109/MC.2010.35 [Accessed: 2022-09-15]

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014a). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, *22*(1). Retrieved from: https://doi.org/10.1108/IMCS-08-2012-0045 [Accessed: 2022-09-15]

Sommestad, T., Karlzén, H., & Hallberg, J. (2014b). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, *23*(2), 200-217. Retrieved from: https://doi.org/10.1108/ICS-04-2014-0025 [Accessed: 2020/07/08]

South African Banking Risk Information Centre. (2021). *SABRIC Annual Crime Statistics 2021* (Annual Crime Statistics. [Online] Retrieved from: https://www.sabric.co.za/media/5dlnhnyj/sabric-crime-stats-2021_fa.pdf [Accessed: 2023-05-04]

Statistics South Africa. (2021). *General Household Survey*. Retrieved from https://www.statssa.gov.za/publications/P0318/P03182021.pdf [Accessed: 2021-05-08]

Surfshark. (2022). *Cybercrime Statistics*. Retrieved from:https://surfshark.com/research/data-breach-impact/statistics [Accessed: 2023-05-26]

Sutherland, E. (2017). Governance of cybersecurity - The case of South Africa. *African Journal of Information and Communication*, *20*, 83-112. Retrieved from: https://doi.org/10.23962/10539/23574 [Accessed: 2022-09-15]

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (Vol. 6).Boston, MA: Pearson [Online] Retrieved from:https://ebook.upgrisba.ac.id/ebook/komputer-informasi-referensi-umum/6th-edition-using-multivariate-statistics-pearson/download [Accessed: 2023-04-12]

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management*, *12*(3), 1-23. Retrieved from: https://doi.org/10.5539/ijbm.v13n6p1 [Accessed: 2023-02-12]

University of Pretoria. (2007). *Code of Ethics for Research*. University of Pretoria. [Online] Retrieved from: https://www.up.ac.za/media/shared/6/files/rt-429-99-university-of-pretoria-code-of-ethics-for-research.zp158366.pdf [Accessed: 2020-07-01]

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *African Journal of Information and Communication*, *20*, 113-132. Retrieved from: https://doi.org/10.23962/10539/23573 [Accessed: 2022-02-12]

van Vuuren, J. J., Grobler, M., Leenen, L., & Phahlamohlaka, J. (2014). *Proposed Model for a Cybersecurity Centre of Innovation for South Africa*. ICT and Society. Berlin, Heidelberg,pp. 293-306.Springer Berlin Heidelberg. 2014.[Online] Retrieved from: https://link.springer.com/chapter/10.1007/978-3-662-44208-1_24 [Accessed: 2022-09-10]

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3), 190-198. Retrieved from: https://doi.org/10.1016/j.im.2012.04.002 [Accessed: 2022-02-12]

Veerasamy, N., Mashiane, T., & Pillay, K. (2019). *Contextualising Cybersecurity Readiness in South Africa*. 14th International Conference on Cyber Warfare and Security. Stellenbosch, South Africa,pp. Council for Scientific and Industrial Research (CSIR). [Online] Retrieved from: http://hdl.handle.net/10204/11247 [Accessed: 2023-02-12]

Weston, R., Gore, P. A., C., F., & Catalano, D. (2008). An Introduction to Using Structural Equation Models in Rehabilitation Psychology. *Rehabilitation Psychology*, *53*(3), 340-356. Retrieved from: https://doi.org/10.1037/a0013039 [Accessed: 2023-02-12]

Wheaton, B., Muthén, B., Alwin, D. F., & Summers, G. F. (1977). Assessing reliability and stability in panel models. *Sociological methodology*, *8*, 84-136. Retrieved from: https://doi.org/10.2307/270754 [Accessed: 2023-02-12]

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research*, *22*(9), N.PAG-N.PAG. Retrieved from: https://doi.org/10.2196/23692 [Accessed: 2023-02-12]

Wirth, A. (2020). Cyberinsights: COVID-19 and What It Means for Cybersecurity. *Biomed Instrum Technol*, *54*(3), 216-219. Retrieved from: https://doi.org/10.2345/0899-8205-54.3.216 [Accessed: 2023-02-12]

Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816. Retrieved from: https://doi.org/10.1016/j.chb.2008.04.005 [Accessed: 2022-02-12]

World Economic Forum. (2023). *The Global Risks Report 2023*. [Online] Retrieved from: https://www.weforum.org/reports/global-risks-report-2023/digest [Accessed: 2023-05-05]

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems*

Education, *23*(4), 407-415. Retrieved from: https://core.ac.uk/download/pdf/301384551.pdf [Accessed: 2022-02-12]

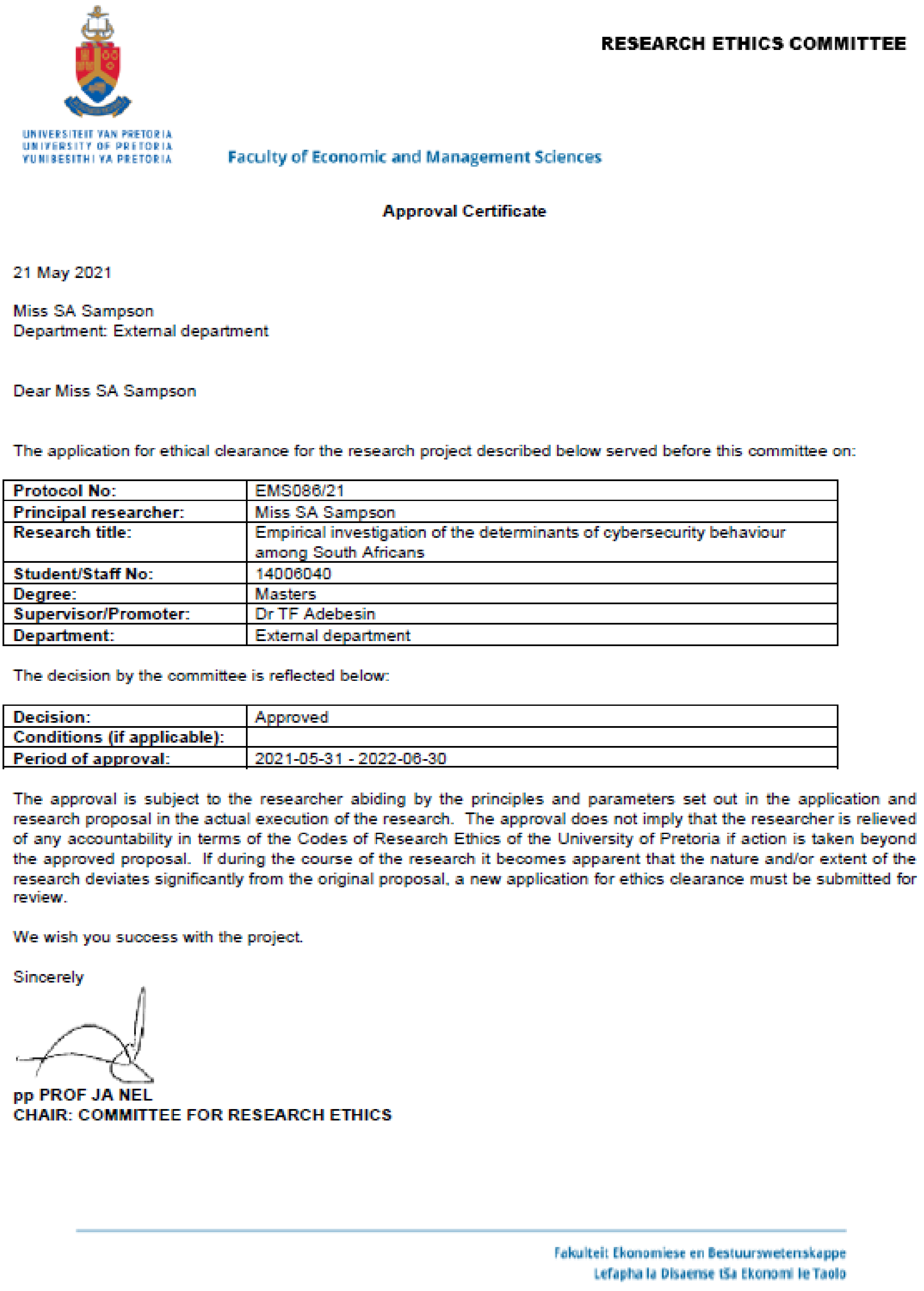
Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, *26*(4), 401-419. Retrieved from: https://doi.org/10.1108/ITP-12-2012-0147 [Accessed: 2022-05-26]

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330-340. Retrieved from: https://doi.org/10.1108/09685220910993980 [Accessed: 2020-07-17]

Zijlstra, W. P. (2009). *Outlier detection in test and questionnaire data for attribute measurement* Ridderprint. Ridderkerk. https://pure.uvt.nl/ws/portalfiles/portal/1158011/3710316.pdf

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*, 1-16. Retrieved from: https://doi.org/10.1080/08874417.2020.1712269 [Accessed: 2022-02-12]

Appendix A Ethical clearance



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

RESEARCH ETHICS COMMITTEE

Faculty of Economic and Management Sciences

Approval Certificate

21 May 2021

Miss SA Sampson
Department: External department

Dear Miss SA Sampson

The application for ethical clearance for the research project described below served before this committee on:

Protocol No:	EMS086/21
Principal researcher:	Miss SA Sampson
Research title:	Empirical investigation of the determinants of cybersecurity behaviour among South Africans
Student/Staff No:	14006040
Degree:	Masters
Supervisor/Promoter:	Dr TF Adebesin
Department:	External department

The decision by the committee is reflected below:

Decision:	Approved
Conditions (if applicable):	
Period of approval:	2021-05-31 - 2022-06-30

The approval is subject to the researcher abiding by the principles and parameters set out in the application and research proposal in the actual execution of the research. The approval does not imply that the researcher is relieved of any accountability in terms of the Codes of Research Ethics of the University of Pretoria if action is taken beyond the approved proposal. If during the course of the research it becomes apparent that the nature and/or extent of the research deviates significantly from the original proposal, a new application for ethics clearance must be submitted for review.

We wish you success with the project.

Sincerely

pp PROF JA NEL
CHAIR: COMMITTEE FOR RESEARCH ETHICS

Fakulteit Ekonomiese en Bestuurswetenskappe
Lefapha la Disaense tša Ekonomi le Taolo

Appendix B Research instrument

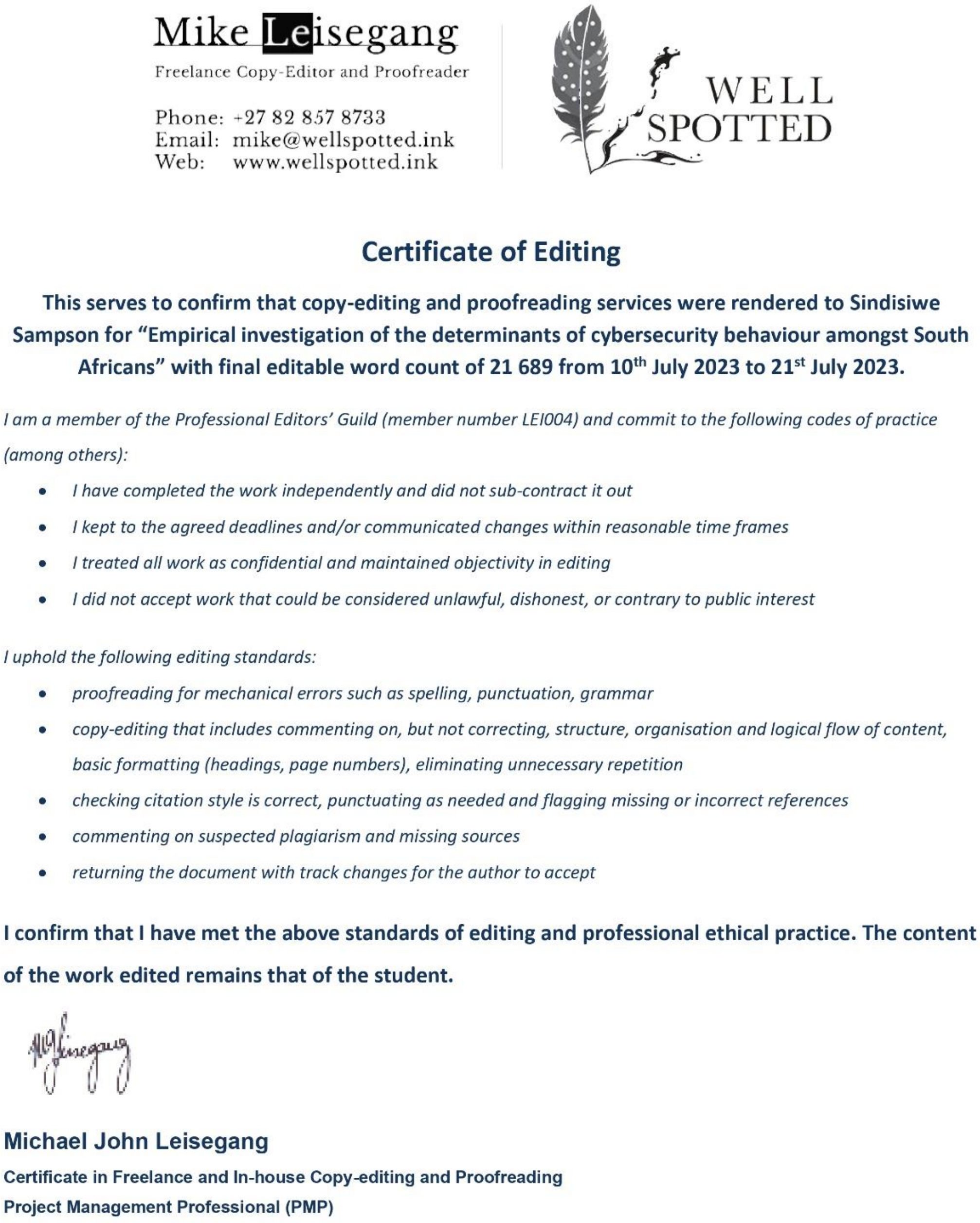
	Strongly Disagree	**Disagree**	**Neither agree or disagree**	**Agree**	**Strongly agree**
Attitude towards cybersecurity behaviour [Anderson & Agarwal, 2010] Cronbach's alpha = 0.88					
1. Security measures such as implementing antivirus software, firewalls, or system updates on my devices (computer, smartphone, or tablet) are a good idea					
2. Practising recommended cybersecurity behaviours (such as using an antivirus / firewall or updating my device software frequently) to protect my devices (smartphone, computer, or tablet) is important.					
3. I like the idea of practising recommended cybersecurity behaviours (e.g. using a strong password or being aware of phishing emails) to secure my devices (smartphone, computer, or tablet) and information.					
Behavioural intention [Dinev & Hu, 2007] Cronbach's alpha = 0.83					
4. I intend to periodically use protective solutions like antivirus software, spam filters, and firewalls to protect my devices (smartphone, computer, or tablet) from malicious software (virus, malware, spyware).					
5. In the immediate future, I intend to change the privacy and security settings on my Internet browser to prevent malicious intrusion on my devices (smartphone, computer, or tablet).					
6. I intend to periodically check the privacy and security settings on my Internet browser to prevent malicious intrusion on my devices (smartphone, computer, or tablet).					
Subjective norms [Dinev & Hu, 2007] Cronbach's alpha = 0.86					
7. Most people who are important to me think it is a good idea to practise recommended cybersecurity behaviours (e.g.. using firewalls or using a strong password).					
8. Most people who are important to me think it is a good idea to prevent cyberattacks by practising recommended cybersecurity behaviours (e.g. not sharing confidential information online).					

	Strongly Disagree	**Disagree**	**Neither agree or disagree**	**Agree**	**Strongly agree**
Perceived vulnerability [Workman, Bommer, Straub, 2008] Cronbach's alpha = 0.854					
9. My confidential information is vulnerable to security violations or illegal access.					
10. I believe that trying to protect my confidential information is likely to reduce illegal access to it.					
11. The likelihood of someone getting my confidential information without my consent or knowledge is high.					
12. The likelihood of someone damaging my system on my devices (smartphone, computer, or tablet) is high.					
13. The likelihood of an information security violation/ cyberattack occurring to me is high.					
Perceived severity [Workman et al., 2008] Cronbach's alpha = 0.974					
14. I believe that protecting my confidential information is important.					
15. Threats to the security of my confidential information are severe.					
16. Having my personal information accessed by someone without my consent or knowledge is a serious problem for me.					
17. Having someone successfully attack and damage the operating systems on my devices (smartphone, computer, or tablet) is severe.					
18. Cyberattacks on my devices (smartphone, computer, or tablet) and information stored on my devices are severe.					
Self-efficacy / Perceived behavioural control [Workman et al., 2008] Cronbach's alpha = 0.929					
19. For me, practising the recommended cybersecurity behaviours is hard (such as updating my device software, using strong passwords, not posting my confidential information online).					
20. I have the necessary skills to protect myself from information security violations / illegal access to my information, data or devices (smartphone, computer, or tablet).					

	Strongly Disagree	**Disagree**	**Neither agree or disagree**	**Agree**	**Strongly agree**
21. I have the skills to implement the available preventative measures (such as using an antivirus/firewall, updating my device software, not falling for phishing emails) to stop people from illegally gaining access to my confidential information.					
22. I have the skills to implement the available preventative measures (e.g.. using an antivirus/firewall, using strong passwords, and not using unsecured Wi-Fi hotspots) to stop people from damaging the operating systems on my devices (smartphone, computer, or tablet).					
23. My skills on what is required to stop information security violations/illegal access to my information, data or devices (smartphone, computer, or tablet) are adequate.					
Response efficacy [Workman et al., 2008] Cronbach's alpha = 0.913					
24. Efforts to keep my confidential information safe are effective.					
25. The effectiveness of available measures (such as not posting my confidential information online, not falling for phishing emails etc.) to protect my confidential information from being illegally accessed/used is effective.					
26. The preventative measures available to me (such as antivirus, strong passwords, not posting my confidential information online, not falling for phishing emails etc.) to stop people from getting my confidential information are sufficient.					
27. The preventative measures available to me (such as using an antivirus/firewall, updating my device software etc.) to stop people from damaging my systems on my devices (smartphone, computer, or tablet) are sufficient.					
28. The preventative measures (such as using strong passwords, not posting my confidential information online, not falling for phishing emails) available to keep people from violating my information security are sufficient.					
Response cost [Workman et al., 2008] Cronbach's alpha = 0.793					

	Strongly Disagree	**Disagree**	**Neither agree or disagree**	**Agree**	**Strongly agree**
29. The inconvenience to practise recommended cybersecurity behaviours (such as using an antivirus / firewall, updating my device software, using strong passwords etc.) outweighs the benefits.					
30. The cost to practise recommended cybersecurity behaviours (e.g.. using an antivirus / firewall, updating my device software, using strong passwords etc.) outweighs the benefits					
31. The impact on my life from practising the recommended behaviours (such as updating my device software, using strong passwords, not posting my confidential information online, not falling for phishing emails) outweighs the benefits					

Appendix C Certificate of editing



Mike Leisegang
Freelance Copy-Editor and Proofreader

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

WELL SPOTTED

Certificate of Editing

This serves to confirm that copy-editing and proofreading services were rendered to Sindisiwe Sampson for “Empirical investigation of the determinants of cybersecurity behaviour amongst South Africans” with final editable word count of 21 689 from 10th July 2023 to 21st July 2023.

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

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

I uphold the following editing standards:

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

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

Michael John Leisegang
Certificate in Freelance and In-house Copy-editing and Proofreading
Project Management Professional (PMP)