University of Fort Hare

Together in Excellence

A framework for cyber safety awareness amongst first-year students in the Eastern Cape, South Africa

by

Everjoy C Makazhe

201820467

Dissertation

Submitted in fulfilment of the requirements for the degree

Master of Commerce

In

Information Systems

In the

Faculty of Management and Commerce

of the

University of Fort Hare

Supervisor: Prof R Piderit

Co-supervisor: Mr M Mamba

Co-supervisor: Dr E Chindenga

May 2025

Abstract

Technology has impacted every part of our daily lives and supports different activities ranging from communications, games, trade and commerce. Students also benefit from social networks, enabling quicker access to information and communication. The outbreak of Covid-19 resulted in a transition from traditional learning to online learning. However, the online learning environment brought a surge in cyber hazards, threats and assaults. In light of this, a cyber safety framework for first-year university students in the Eastern Cape of South Africa was required.

The pragmatism research paradigm influenced the study, resulting in a quantitative research design selection. Online surveys created on the Survey Monkey platform were used to collect data. Several closed-ended questions used a Likert scale with a score of four (4). Microsoft Excel and the Statistical Package for Social Sciences (SPSS) were used for data analysis and display. Experts then reviewed the proposed framework in the field to evaluate its suitability for the higher education context. The feedback was incorporated into the final framework proposed by this study.

The study's results revealed that university students' main online risks were cyber bullying, phishing scams, identity fraud, invitations to pornography and sexting. The more time the students spend online, the more online risks they face. The study's findings further showed that the level of cyber security knowledge leads to cyber safety awareness among first-year students in Eastern Cape. Research findings indicated that there are mixed cyber security attitudes, which affect cyber safety awareness. The factors required to develop the framework include attitude, risk, time, awareness and knowledge capacitation. Based on the study's findings, future research can use a sequential mixed methods approach to determine the views of key informants from universities, service providers and even parents on the different measures they provide to ensure cyber safety.

Key words: cyber safety awareness, Eastern Cape, framework students, online risks

Declaration of Originality

I, Everjoy Chipo Makazhe, hereby affirm that:

- The work in this dissertation is entirely original to me and has never before been presented in full or in part to satisfy the criteria for a higher or equivalent degree at another University.
- I am completely aware of the University X's anti-plagiarism policy, and I considered all necessary steps to abide by the rules.
- The University X's policy on research ethics is something I am completely aware of, and I have made all reasonable steps to adhere to the rules. My reference number is PID011SMAK01. I have a certificate of ethical approval from the University X's Research Committee (Appendices 1 and 2).

Signature: _____Makazha_____

Date: _____28 February 2025_____

Acknowledgments

I want to thank God for giving me the strength to endure the struggle and finish my dissertation.

I want to express my sincere gratitude and appreciation to my supervisor, Prof. Roxanne Piderit, and co-supervisors, Mr Mamba and Dr E. Chindenga, for their invaluable guidance, coaching, support, and encouragement throughout this study as well as for ensuring the completion and submission of this dissertation.

For the financial support, I also wish to acknowledge the University Y and the Govern Mbeki Research Development Centre (GMRDC) at the University X.

I am grateful that the University X and University Y students took the time to complete the online survey. Along with them, I thank the proof reader for reading my work and making insightful and helpful recommendations.

I want to thank my parents, my husband, Dr M.G. Bomvu, my kids, and all of my friends for their unfailing encouragement, understanding, and support during my Master's degree.

Table of contents

List of figures

List of tables

CHAPTER 1

OVERVIEW OF THE RESEARCH STUDY

1.1 Background of the study

Technology has impacted all aspects of our lives, from socialization, productivity, transport, healthcare, etc.; however, this study focuses on learning in higher education institutions. Over the last few years, there has been a rise in internet bandwidth, wireless technologies, and related infrastructure, making Africa one of the upcoming markets for information technology (Bada et al., 2019; Matyokurehwa et al., 2020). Due to growing accessibility, more students now have access to technology, including mobile phones, tablets, laptops, and desktops (Alzubaidi, 2021). Students also benefit from social networks and quicker access to information and communication, which has become rapid (Kovacevic & Radenkovic, 2020). Today, students are more likely to have access to information and communication technology (ICT) devices and an internet connection at home. More institutions are using ICTs to improve education (Moallem, 2019). According to Kritzinger (2017), ICTs have brought along significant benefits for teaching and learning, such as increased interaction and student engagement, accessibility of learning at any time and offering new learning methods.

Despite the numerous benefits of ICTs for education, the majority of educational institutions around the world, including those in South Africa, still use traditional teaching and learning methods which involve face-to-face interactions and direct physical contact (Tick et al., 2021). However, the Covid-19 pandemic caused a change in how teaching and learning are facilitated globally, and South Africa has not been exempted from the emergent changes. Most academic institutions have shifted to online learning, while other institutions have resorted to blended learning, including both online (e-learning) and physical classes. Due to the Covid-19 pandemic and the subsequent closure of schools and universities, internet usage increased by 50% (UNICEF, 2020). Using blended or wholly online means of learning meant that the educators and students spent most of their time online. This increased the probability of the students being exposed to challenges associated with over-access to online technologies.

As the epidemic lingered longer, most academic institutions were concerned about accessibility, cost, flexibility, learning pedagogy, lifelong learning, and regulation of online

learning (Dhawan, 2020). The Covid-19 pandemic also caused an increase in a secondary major threat to a technologically advanced society, such as a series of random and several targeted cyber attacks and cyber crime campaigns (Lallie et al. 2021). The Covid-19 epidemic, however, has given more attention to the implementation of online learning than it has to the online risks students will face while learning online.

The abrupt transition from traditional learning to online learning that the COVID-19 epidemic brought about caught higher education institutions off guard (Mncedisi et al., 2021). In South Africa, twenty-six (26) public higher education institutions are spread among its nine (9) provinces. There are six (6) technical universities, nine (9) comprehensive universities, and eleven (11) ordinary academic institutions (Patrick et al., 2021). In response to COVID-19, South African institutions have prioritised using a learning management system (LMS) as a crucial element of distance education (Dlamini & Ndzinisa, 2020). Zoom, Microsoft Teams, and Skype are frequently used platforms for online conferences, video meetings, and webinars (Patrick et al., 2021). Lecturers should be cognizant of the pre-existing cultural categorization as South Africans from many socioeconomic backgrounds participated in the COVID-19 lockdown (Gumede & Badriparsa, 2022). Universities have had to spend significantly on digital technology to adopt online learning and keep up with the speed of changes. Since the state-wide lockdown, students have had access to online learning resources, but many have depended on the government for free cell phones, tablets, PCs, and data (Laher et al., 2021). Universities reopened for the academic year on digital internet platforms on the 20th of April 2020. The universities were supported by agreements with telecommunications providers to offer free bandwidth to all students. Additionally, websites with zero-data ratings were developed to support online education and remote teaching (Pillay et al., 2021).

Several universities went so far as to buy computers to lend to students to guarantee that students could access online learning platforms. Still, some students have been unable to complete their learning objectives due to inadequate preparation and insufficient access to digital learning resources (Dlamini & Ndzinisa, 2020). It should be highlighted that the distribution of digital technology to students and university employees has been a priority for universities and the South African government, with less focus on students' online safety.

Although there have been increases in access to information technologies for students, there is also an increase in online predators engaged in several illegal and unethical activities (Kritzinger et al., 2017). Due to the Covid-19 pandemic, more people than ever are relying on digital tools to promote children's play, learning, and socialization. Digital solutions offer enormous opportunities for upholding and promoting student rights but may also expose students to more online threats (UNICEF, 2020). Many educational institutions employed Google Classroom, Zoom, and other remote learning tools to allow students to continue their education once traditional learning was suspended (Mpungose, 2020). As people increase their time online, societies face significant security and privacy challenges (Mishna et al., 2010). The Internet creates a borderless world, exposing users to several threats. These threats happen everywhere, regardless of space, such as in schools or the workplace (Asanan et al., 2017). Kritzinger et al. (2017) show that children between the ages of fifteen (15) and sixteen (16) spend almost five (5) hours per day online. As people spend more time online, about 25% are likely to become cyberbullying victims (Mishna et al., 2010). With this being said, this study has proposed a framework for cyber safety awareness based on first-year students in the Eastern Cape region of South Africa. Internet users must be aware of their security and safety online to decrease the number of cybercrime victims (Senthilkumar & Easwaramoorthy, 2017). There is a need to comprehend university student’s awareness of cyber safety in this regard.

There is also a need to understand how students behave online since they might not know how to safeguard themselves if they are not technology specialists (Rotas and Cahapay, 2021). While there are ways to lessen the difficulties that internet users experience by limiting and preventing their use, it is imperative to keep users aware of their hazards daily (Potgieter, 2019). Due to a lack of awareness about this topic, many believe that being aware of cyber safety is unnecessary (Asanan et al., 2017; Catota et al., 2019). The studies which have been done, especially during the Covid-19 were on the challenges of online learning (Dlamini & Ndzinisa, 2020; Mukuna & Aloka, 2020), remote learning experiences of students (Gumede & Badriparsa, 2022; Mncedisi et al., 2021; Pillay et al., 2021), and the institutional response to Covid-19 (Salami, 2021; Thaba-Nkadimene, 2020). This indicates that little to no attention has been paid to how the growing usage of online learning platforms has impacted students' online conduct. Studies such as this are required to ascertain the level

of cyber safety knowledge among first-year students at University X and the University Y in the Eastern Cape of South Africa.

This chapter, organized within the backdrop of the study, largely included the first-year student's experiences in the Eastern Cape province of South Africa, with cyber safety awareness. The problem statement, objectives, and research questions that serve as the study's compass are further described in this chapter. The researcher further highlights the research hypothesis, the importance of the study, preliminary literature evaluation, theoretical framework, and research methodology in this chapter.

1.2 Problem Statement

South Africa lacks information on online safety awareness compared to Africa and its international counterparts (Chandarman & van Niekerk, 2017). Within the South African context, Chandarman and van Niekerk (2017) indicated a need to have targeted cyber safety awareness campaigns dealing with the shortcoming of a specific population of users. Walaza et al. (2014) stated that, while focusing on the students, there is a shortage of ICT security information in South African education. This is further worsened by the fact that no curriculum caters to cyber safety education (Waldock et al., 2022). The students with access to cybersecurity education are those with computer-related degrees. This means that there is limited or no education about cyber safety awareness for students coming from high school, which exposes them to more cyber threats online. More so, Catota et al. (2019) indicated a necessity to comprehend the amount of cyber awareness in large, diverse groups. There is little knowledge of cyber safety awareness amongst first year students, and this study explored the practices underway based on first-year students' experiences. In light of the dearth of cyber safety knowledge in a nation like South Africa, this study proposed a framework for first-year students in the Eastern Cape province of South Africa for the benefit of lecturers, decision-makers, and institutions, as well as the students.

1.3 Research questions

To address the problem statement, the following research questions were derived:

What measures can be used to reduce the cyber safety awareness challenges faced by first year students in the Eastern Cape?

The main research question was split into four relevant sub-questions:

1. What is the association between online time and the hazards faced by first year students at a selected university in Eastern Cape?

There are several online risks that first-year students face at a global level. The risks faced by the students vary based on the amount of time spent online, online behaviour, and the knowledge and attitude of the students towards cyber safety. Some common online risks were spam mail, malware, suspicious websites and domains, attacks from Distributed denial of service (DDoS), and social media messaging (Wang & Alexander, 2021). Sexting is another form of online risk that can be done by a stranger, friend, or acquaintance by sending or receiving sexual images, videos, and texts online. This is also classified as a form of sexual solicitation. Sexual solicitation usually leads to risky sexual behaviour online. Students that engage in online activities have the danger of being exposed to content risks, contact risks, economic risks, and privacy hazards (Al-Badi et al., 2016; Schilder et al., 2016). Cyberbullying, communicating with strangers, sending embarrassing photos, sharing their location publicly, and spreading risky pranks and games are just a few of the online risks that students may encounter when they are online (Beverley & Covey, 2018; Paluckait & Ardeckait-Matulaitien, 2016). The exposure of university students to online risks worsened due to the COVID-19 pandemic, which made universities globally and in South Africa adopt online learning. When the pandemic receded, face-to-face and online learning (blended learning) were adopted. According to Zahidah et al., (2020), the more one spends online, the higher the likelihood of facing online threats. Moreso, there is a psychological need for one to remain connected online due to several reasons, which further makes the end user more exposed to online risks (Quayyum et al., 2021).

2. How does cyber security knowledge affect cyber safety awareness among first-year students in the Eastern Cape?

There is a misconception among internet users that if someone uses a unique password, one is protected and is no longer vulnerable to threats. Although it’s a significant good step to create unique passwords, it is not enough to keep the user's information private due to hackers having knowledge and technologies which can decrypt passwords or do a password bypass (Hunt, 2016). Cyber security awareness is a good mitigation measure against online attacks

that a user can face (Garba et al., 2020). cyber knowledge is about risk management, which implies that the student or online or technology has to develop a perception of risk such that there can be the development of need to mitigate the perceived risk again. Thus, the perception of risk leads to the development of protective behaviour of the technology used. However, cyber safety knowledge does not necessarily translate into cyber safety awareness. Students can be conscious of their actions, although they are unaware of their data being used elsewhere within and between university systems (Alqahtani, 2022a). A study in Nigeria found that students had a basic knowledge of cyber security. Still, they were unaware of what to do with the knowledge they had to secure themselves (Alharbi & Tassaddiq, 2021). The availability of knowledge translates to the end user not becoming a victim of cyber threats. However, people still fall victim to phishing attacks despite being knowledgeable about them (Rajan, 2010). The reason for that could be incorrect behaviour towards online security (Chandarman & van Niekerk, 2017).

3. What is the effect of cyber security attitude on cyber safety awareness of first-year students in the Eastern Cape?

Personal attitudes towards online behaviour in users could be influenced by information security awareness (Vafaei-Zadeh et al., 2019). In this case, user awareness of threats in an information technology context is one of the main predictors of attitude. Information security awareness can increase the user's security precautions, and eventually, individuals will have a more positive attitude. An individual's desire to engage in behaviour should be higher the more favourable the attitude, and the subjective norm is toward the behaviour and the larger the perceived behavioural control (Festl et al., 2013). Information security awareness is expected to influence the attitude towards having more intention regarding using anti-malware software. The theory of planned behaviour Ajzen & Fishbein, (1980); Ajzen, (1991) contends that subjectively perceived standards are crucial in explaining specific types of behaviour. These factors, along with the person's attitude toward the behaviour and the perception of behavioural control, affect the intention to engage in the suggested behaviour (Festl et al., 2013).

4. What measures can be developed to address cyber safety awareness challenges among first-year students in Eastern Cape?

The training also debunks the misconception that the installation of anti-virus is enough to protect their electronic gadgets and that firewalls are synonymous with anti-virus Mishna et al., (2010). One strategy is to raise risk awareness, for instance, through educational materials and behaviour-related information (Prochaska et al. 1998). Both models emphasize the significance of education and awareness campaigns to encourage behavioural change, in this case, to lessen risky internet behaviour. Thus, it appears that there is a rising need for an obligation on the part of institutions to provide instructional and preventative initiatives about harmful Internet use. Gaming can draw students toward the risks associated with online learning and social media networks. Ticket al. (2021) suggested that games can be used to increase digital literacy. Although students' grasp of the digital world has improved with time and exposure, it is far from assured that this awareness will translate into caution when safeguarding personal information. There is no one size fits all for the measures that can be used to deal with students' daily learning of cyber crimes. Generally, the idea is to keep the students aware of the risks they face in online learning.

1.4 Objectives of the study

The study's main objective was to develop a framework for cyber safety awareness amongst first year students in the Eastern Cape, South Africa.

1.4.1 Secondary objectives

1. To determine the association between online time and the hazards faced by first year students at a selected university in Eastern Cape
2. To determine the effect of cyber security knowledge on cyber safety awareness among first year students in Eastern Cape
3. To examine the effect of cyber security attitude on cyber safety awareness of first year students in Eastern Cape
4. To develop measures for addressing cyber safety awareness challenges among first year students in Eastern Cape

1.4.2 Research hypotheses

The research will test the following hypotheses for the study:

1. H_o At selected universities in the Eastern Cape, there is no connection between online time and the hazards that first-year students confront.

   H_1 There is a significant association between online frequency and online risks faced by first year students at selected universities in the Eastern Cape.

2. H_o There is no significant association between cyber security knowledge on cyber safety awareness among first year students at selected universities in the Eastern Cape.

   H_1 There is a significant association between cyber security knowledge on cyber safety awareness among first year students at selected universities in the Eastern Cape.

3. H_o There are no effects of cyber security attitude on first year students' cyber safety awareness at selected Eastern Cape universities.

   H_1 There are effects of cyber security attitude on first year students' cyber safety awareness at selected Eastern Cape universities.

The hypotheses above can be made into a conceptual framework used in the study.

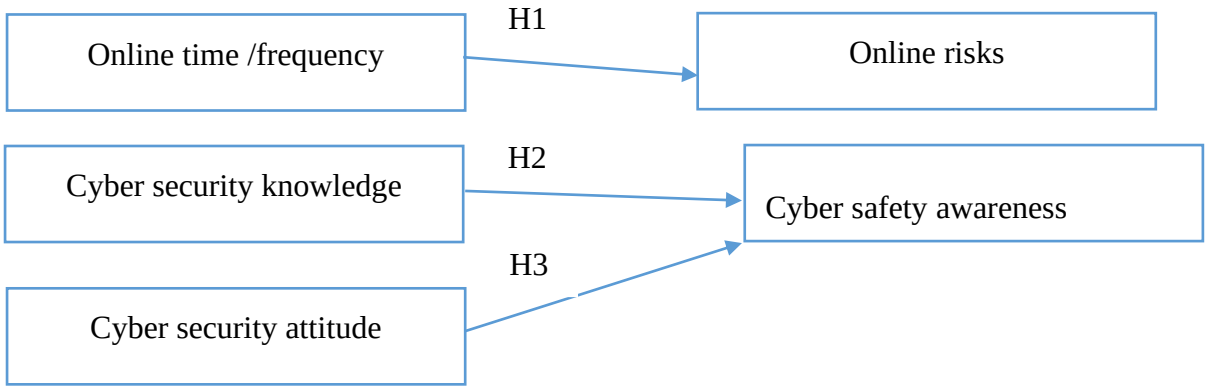


Figure 1.1: Conceptual framework for hypothesis development

The human behaviour of the students was as a result of their online frequency which would lead to their online risk (Figure 1.1). The cyber security knowledge that the students had (risk perceptions, practicing safe use of the internet) which would mean that they had to change their passwords, install firewalls and reduce their levels of trust (see Figure 4.3). The level of trust when online can be changed through training and thereby changing their cyber security attitudes which would mean that their cyber safety was increased.

For the researcher to clearly show the linkages between the elements of the study, a research matrix was adopted as shown in Table 1.1. The methodological research matrix presented the objectives and the research questions of the study and the appropriate research design for each of the objectives and the anticipated results. It is from each of the objectives and the research questions that conclusions would be made. Specifically, the objectives and the conclusions will be matched one for one meaning that objective 1 will be related to the results 1 and then the same will be concluded under conclusion 1.

Table 1.1: Methodological research matrix

Objectives	Research question	Research design	Results	Conclusions
1. To determine the association between online time and the hazards faced by first year students at a selected university in Eastern Cape	*1. What is the association between online time and the hazards faced by first year students at a selected university in Eastern Cape?*	Quantitative	*Main online risks that university students faced were cyberbullying, phishing scams, identity fraud, invitations to pornography and sexting. Time spent online is significantly associated with the likelihood of facing online risks.*	*The students are faced with several online risks. The more time the students spend online, the more online risks they face.*
2. To determine the effect of cyber security knowledge on cyber safety awareness among	*2. How does cyber security knowledge affect cyber safety awareness among first-year students in the Eastern Cape?*	Quantitative	*Mixed results, with some students knowledgeable and others not having cyber knowledge about*	*The level of cyber security knowledge leads to cyber safety awareness*

first year students in Eastern Cape			*the different online threats. A statistically significant association between cyber security knowledge and cyber safety awareness among first year students in Eastern Cape*	*among first year students in Eastern Cape*
3. To examine the effect of cyber security attitude on cyber safety awareness of first year students in Eastern Cape	*3. What is the effect of cyber security attitude on cyber safety awareness of first-year students in the Eastern Cape?*	Quantitative method	*Mixed cyber security attitudes affect the level of cyber safety awareness. A statistically significant association between the student's attitude and cyber safety awareness*	*Positive cyber security attitude leads to cyber safety awareness*
4. To develop measures for addressing cyber safety awareness challenges among first year students in Eastern Cape	*4. What measures can be developed to address cyber safety awareness challenges among first-year students in Eastern Cape?*	Sequential mixed method	*Measures to deal with the challenges faced by students were providing training and awareness campaigns, changing passwords frequently, and*	*The factors required for the development of the framework include attitude, risk time awareness and knowledge capacitation*

			having cyber safety aspects included in their curriculum	

1.5 Significance of the study

The use of remote learning by students, parents, teachers, and lecturers has expanded due to Covid-19. Given the current wave of widespread remote learning, it is reasonable to predict that providing students with threat knowledge will enhance their defensive behaviours (Rotas and Cahapay, 2021). Research studies on cyber safety awareness are beneficial. Various elements influence first-year students' knowledge of safe internet and computer usage. These elements include the student's educational background, the parent's understanding of these issues, and internet access restrictions (de Barros & Lazarek, 2018). Therefore, it is essential to research the level of cyber safety awareness of first year students to determine the necessary implementable legislation and measures for cyber safety that can be applied in schools and universities. Given that the students come from various socioeconomic situations, it is important to comprehend how to act to lessen cyber threats. It is also essential to carry out this study for first-year students to understand online behaviour and reduce the challenges in providing cyber safety awareness.

ICT use in schools, colleges, and universities is becoming the standard, and more and more students have access to ICT equipment at school, including cell phones, tablets, and computer labs (Alzubaidi, 2021). All stakeholders must raise awareness of ICT and cyber safety, especially universities that offer or have access to ICT equipment in the learning environment (Matyokurehwa et al., 2020). This provides an understanding of the cyber safety threats faced by students in universities, and the well-being of students online will be protected in the face of increased threats. Thus, after identifying the threats that first-year students face, measures and recommendations were developed to develop a cyber safety awareness framework.

1.6 Literature and theoretical review

To make a useful review of the literature on the subject under study, the researcher looked at journals, books, dissertations and theses by other scholars. From the literature review, there

was an identification of the theory or theories which influenced the study. The literature was used to identify the gaps in knowledge that the study filled in. The discussion of the findings was based on reviewing the research objectives such that areas of agreement and disagreement with the current study were established.

The researcher used the systematic review approach to identify articles to constitute material for literature review. Information systems researchers have been criticised that they are not aware of how literature review can be structured. The researcher followed the Systematic Literature Review (SLR) which was initially targeted for health related studies but can be extended for non-health interventions (Okoli & Schabram, 2010). In this study, the SLR meant that there was a systematic, explicit and comprehensive method which involved identification, evaluation and synthesis of research work. Based on the elements of the SLR, there is need to shift from regurgitating the subject matter but synthesising and providing a balanced critique of the theory (Okoli & Schabram, 2010). This meant that the study consulted both qualitative and quantitative studies to come with a comprehensive outlook towards cybersafety awareness among first year university students at selected universities in South Africa during the COVID-19 pandemic. According to Okoli and Schabram (2010), SLR has an eight-step guide which was followed in the study as it was situated in the context of information systems. However, it should be noted that the SLR was used to set the tone of the research as the aim was to produce a graduate student thesis. Therefore, this was not a stand along literature review. The eight steps followed in this study were presented in Figure 1.2 and these included the purpose of the review, protocol and training, searching for literature, practical screen, quality appraisal, data extraction, synthesis of literature and writing of the review.

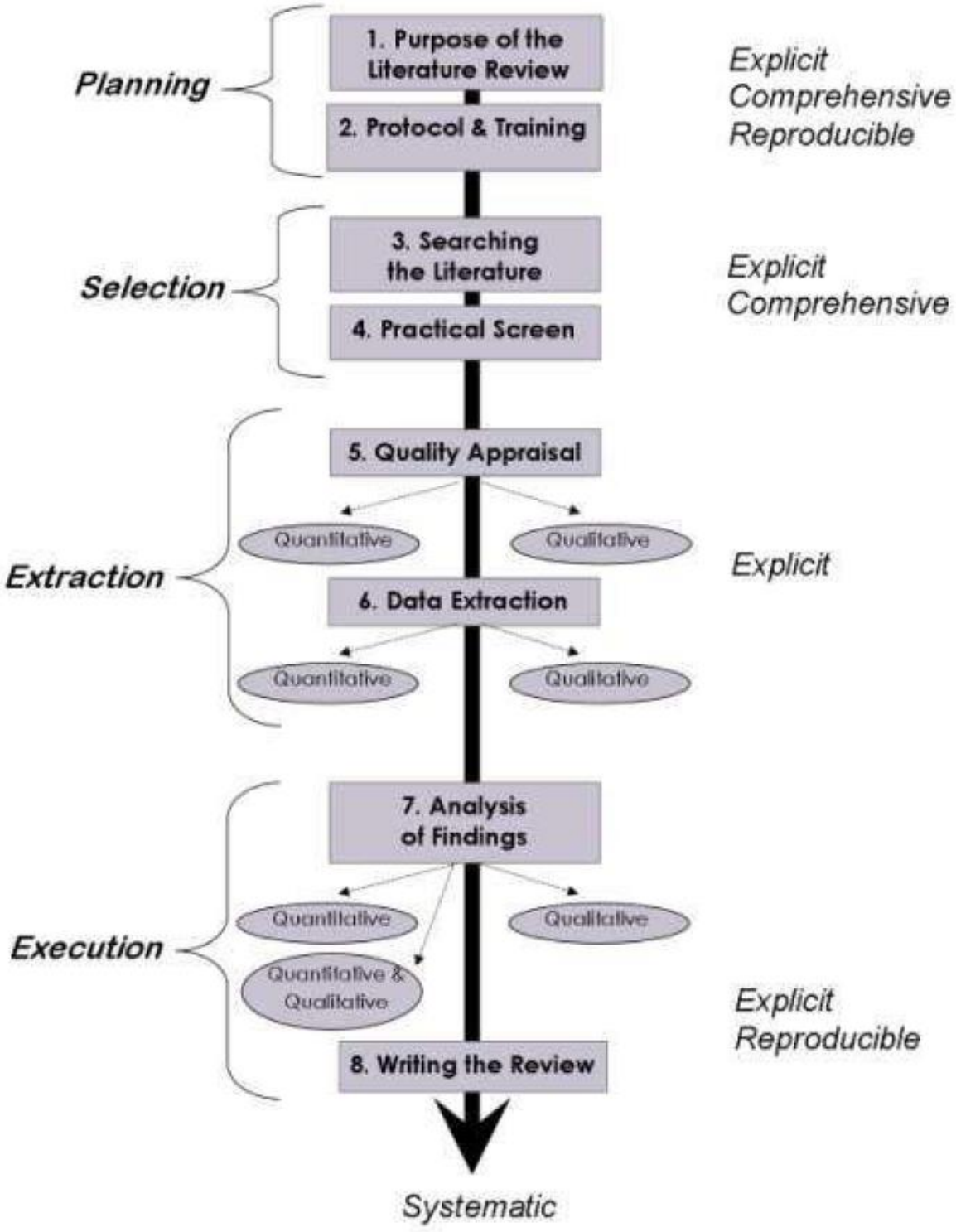


Figure 1.2: Steps followed when carrying out a systematic literature review (Okoli & Schabram, 2010).

I went into detail to explain how each of the steps indicated in Figure 1.2 were followed in this study.

i) Purpose of the literature review

In this step I was clear what the aim of the review was and in this case the aim was to develop a cyber safety framework for first year university students in South Africa. The review also covered the research objectives of the study in order to have global, regional and local view points under different social, economic and political environments. The other objective was to review how the COVID-19 pandemic affected the online presence of students and the challenges which they faced.

ii) Protocol and training

This was an individual research for the purposes of a post graduate thesis and there were no co-authors who needed training on the procedures which needed to be followed to consistently produce the same results. However, my supervisors were the once who gave me guidance on how to carry out the systematic review although they did not receive training. The supervisors made sure that I adhered to the demands of the SLR. The procedure which I followed is from Figure 1.2 on how I went about carrying out the literature review.

iii) Searching for the literature

Following the recommendations by Okoli and Schabram, (2010), I needed to be explicit about how I contacted my search of literature in a way which is as comprehensive as possible. Possible keywords and word combinations were used in the 'abstract, title, keywords and topic' in order to increase the chances of identifying cyber safety awareness studies carried on first year university students. The approach included looking at articles which covered the following keywords: 'cyber safety awareness', 'online', 'COVID-19 pandemic', 'first year university students', 'cyber safety awareness framework' from the Google Scholar database.

iv) Practical screen

Practical screening provided the inclusion criteria which I was supposed to followed in stating the studies which were considered from the review and the ones which were eliminated. The reasons for inclusion and exclusion were also provided by the researcher. The researcher made use of the snowballing approach used by Floress et al. (2019). Under the snowballing approach was used to select references and this is a process in which the

reference section of each article selected were followed up such that fresh articles which met the stated criteria were added to the database (Floress et al., 2019). The snowball approach was used till no new references were identified. Since the study was started in 2021, the researcher chose a 10 year period starting with literature from 2011. Exclusion criteria was for opinion pieces and other grey literature. Included in this study were dissertations which were published at the different websites. A total of 200 articles were identified in the beginning. A total of 70 were reviewed to determine if they met the initial criteria which included being published between 2011 to present (2023), if it's a theory published outside 2011, dealt with cyber safety framework for students in general.

v) Quality appraisal

The articles were judged based on their inclusion in the review and the study reviewed both quantitative and qualitative published literature. The quality of the articles was based on the research methods employed more specifically on relevance, study design, sample size and sampling, data collection, data analysis, ethical considerations and reporting. In this case, the more relevant studies dealt with 1st year students, under the COVID-19 pandemic and how they accessed online material, the time they spend online and the challenges which they faced and the measures which they used to reduce the challenges they faced.

vi) Data extraction

From the researches which were included in the study, the researcher extracted information systematically in line with the objectives of the study. The study managed to collect the theories which influenced the study such as the Theory of Planned Behaviour, Social Learning Theory and National Institute of Standards and Technology (NIST) framework. The researcher also extracted information about the online frequency, cyber awareness knowledge and attitude of the students during the COVID-19 pandemic across the globe. Information also extracted included the challenges faced when online and measure they use to mitigate the challenges. The data also extracted from the review was the critical success factors which affected the cyber safety awareness of university students.

vii) Synthesis of the studies

The study also combined the information collected from the quantitative and qualitative studies or even mixed method studies. The results from the research were used to identify the gaps in knowledge between the previous studies and the current studies.

viii) Writing a review

The research was not a stand-alone review and it provided the theoretical setting for the study. This meant that the systematic review was the grouped into different chapters of the study. For example literature review was made for chapters 2, 3 and 4. Additional material from the systematic review were used to provide a detailed discussion of the findings as a way to show the similarities and differences between the studies.

1.6.1 Theories guiding the study

1.6.1.1 Theory of Planned Behaviour (TPB)

The study was guided by the Theory of Planned Behaviour (TPB) put forward by (Ajzen, 1991). TPB suggests that attitudes and norms the person thinks are subjective and affect the individual's behavioural intent, eventually affecting actual behaviour. An individual's attitude towards a specific behaviour will be based on a negative or positive appraisal of the individual's conduct. Subjective norms will be influenced by the forces around the individual such that there is engagement or non-engagement of a particular behaviour (Burns & Roberts, 2013). The probability of engaging in a specific behaviour is regarded as an individual's intention (Figure 1.2).

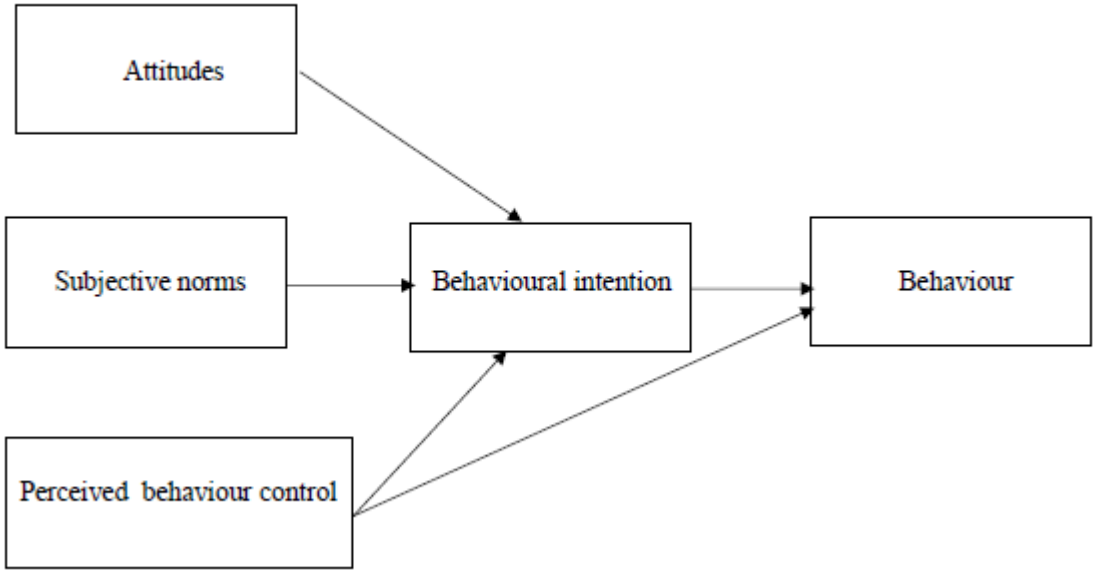


Figure 1.3: Theory of Planned Behaviour: Source:(Ajzen, 1991)

The likelihood of an individual's intention will depend on how closely intention and behaviour are related. According to the TPB, the intention is premeditated regarding its temporary stability. The TPB emphasizes perceived behavioural control (PBC), which influences a person's behaviour. The idea was pertinent to our research since it was necessary to identify the online hazards faced by first-year students at universities in the Eastern Cape. Instead of generalizing them, the research developed strategies for preparing online risk-specific awareness. The TPB was fascinating in the investigation to ascertain the degree of cyber safety knowledge among first-year students in the Eastern Cape. This was based on their attitudes towards the risk behaviour they exhibit when engaging in online activities. Perceived behavioural control was measured in the study by determining the level of cyber safety awareness among first year university students. Thus, the study's findings can be used as a launchpad for schools and policymakers when creating cyber safety awareness strategies. The theory was relevant in this study as it can predict the student’s online behaviour. The researcher recommended the cyber safety awareness measures for the first-year students at University X and University Y in the Eastern Cape from the online behaviour.

1.6.1.2 The Social Learning Theory

Akers put forward the Social Learning Theory (SLT) based on the behavioural learning approach. In theory, there is a utilization of the learnt behaviour and differential association

(Bada et al., 2019). Thus, differential association is related to how people interact and how the associations with different people impact their values and norms (Bhatnagar & Pry, 2020). The first group of people that affect family and friends' behaviour and the associations that happen at an early stage in life tend to last longer, affecting the individual's behaviour. For this concept, there is a relationship with the study because the first-year student's associations affect the individual's behaviour online and the associated challenges. The other concept of the SLT is that of attitude, which implies how a person perceives good and bad (Gabra et al., 2020) and specifically to the study, it refers to how an individual views online behaviour and the awareness towards cyber safety for the first year students at selected universities in Eastern Cape. The other component of the SLT is differential reinforcement, which means the gains and losses associated with some behaviour. Imitation is another concept of the SLT, which implies observing some behaviour and imitating the individual's behaviour. In this study, the individual can imitate online behaviour and also the cyber safety measures which can be copied or not copied. Overall, the SLT will be used in this study to explain the variability in online behaviour and level of cyber safety awareness.

1.6.2. Empirical literature

The global picture of cyber safety awareness from various countries was used to discuss the literature. Literature is discussed to show the different levels of awareness due to policies and socio-economic development differences. The section on literature also discussed the theories guiding the study, namely the Social Learning Theory and the Theory of Planned Behaviour. The theories were a source of the relationship between cyber safety knowledge and attitude toward cyber safety awareness. The literature also discussed how knowledge and attitude affect awareness. The literature discussed the global efforts of dealing with online risks, which led to frameworks such as NIST being developed. An overview of the concepts in this study is discussed below:

1.6.2.1 Cyber safety knowledge

Alqahteni (2022) states that users of digital technologies may be more in danger as they are more thoroughly incorporated into daily life. Cyber security must be considered against shifting technological trends, goods, and behaviours. Cyber safety, also known as online safety, internet safety, e-safety, and digital safety, is widely understood to be the responsible and safe use of Information and Communication Technologies (ICTs).

1.6.2.2 Cyber safety attitude

An attitude toward internet safety may be described as a positive or negative set of assumptions about the topic and its problems (Okanlawon et al., 2015). The term "attitudes" in the context of cyber security refers to a person's point of view, which might affect their conduct online (Antunes et al., 2021). These attitudes, which may influence how a person chooses a certain event on online activity, are the product of their learning experiences, social variables, and observation.

1.6.2.3 Cybersecurity awareness

Awareness is the first step in reducing the number of identity thefts and threats to personal information, which reduces the risk of their information being compromised. One of the key components of information security is awareness, which encourages good security practices and enhances cyberspace security (Vafaei-Zadeh et al., 2019). The amount of awareness and attitude toward cyber security concerns may thus be determined by understanding the hazards a user encounters on the internet.

1.7 Research methodology

Research methodology refers to the strategies employed in a particular study to meet its aims (Bhattacherjee, 2012). Therefore, any methodology seeks to clarify the findings of scientific investigation and the approach itself (Yilmaz et al., 2017). This section gives a general overview of the research philosophy that directed this project, the methods for collecting primary and secondary data, the study's demographic and sample size, and the ethical guidelines that will be followed, as shown in Figure 1.3.

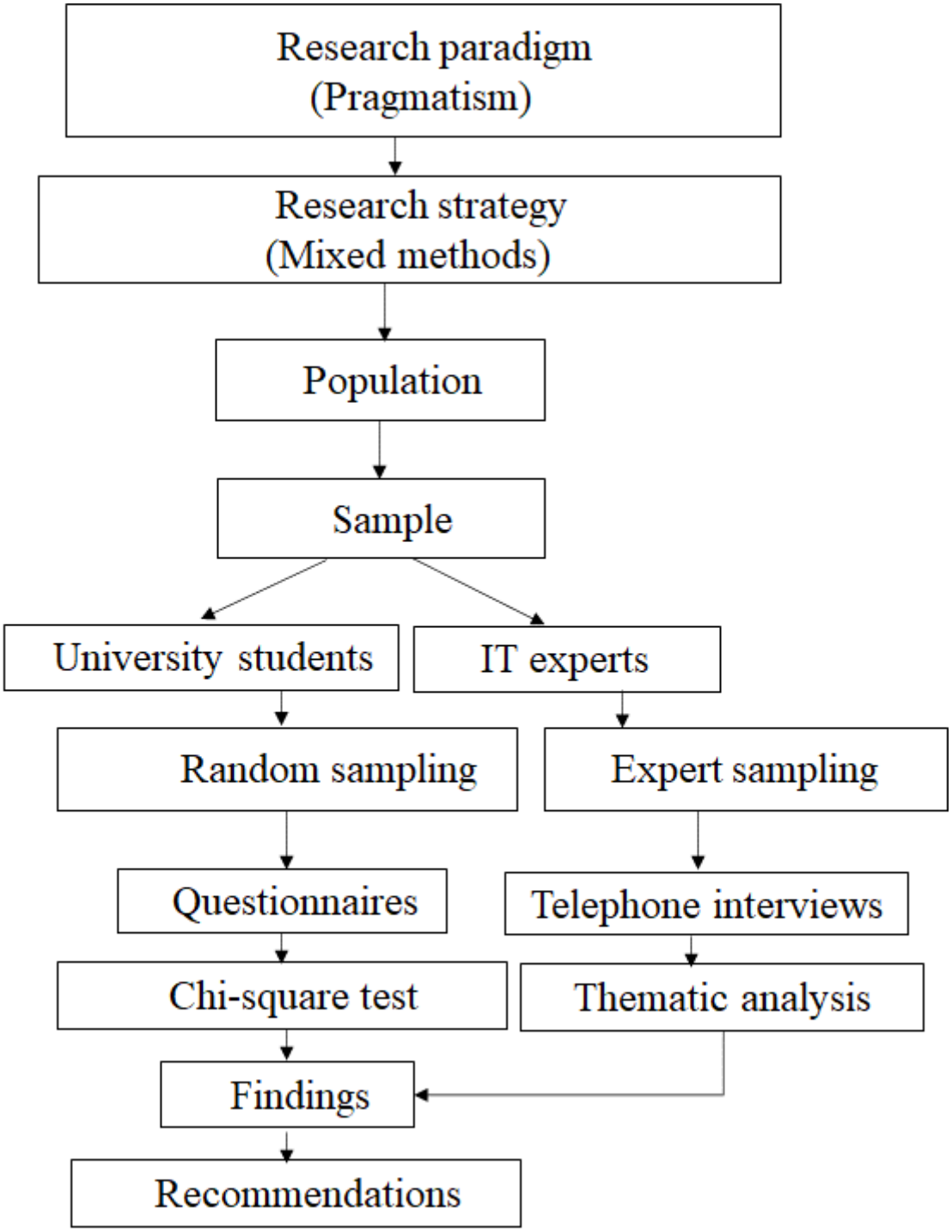


Figure 1.4: Methodology to be used in this study

1.7.1 Research paradigm

The research was predominantly quantitative, as it relied on collecting large datasets as data was collected using questionnaires from first year university students. On the other hand qualitative data was collected using expert interviews. Due to the need to formulate

hypotheses and collect data from experts in computer science or information systems, the researcher adopted pragmatism research paradigm. Since the study was done during the Covid-19 pandemic, online questionnaires were used for quantitative data collection. The research paradigm also influenced the research design to be used in the study. Since the research was carried out during the time of the COVID-19 pandemic, telephone interviews were used to collect data from the experts. Directly related to the pragmatism research paradigm was the quantitative and qualitative research design (explanatory sequential mixed methods research design). An explanatory sequential mixed design is also called a two phase model which consists of collecting quantitative data and later on collect qualitative data which is used to explain the quantitative data (Creswell, 2012). The study adopted the explanatory sequential design which involves collecting quantitative data first, followed by qualitative data to help explain and expand upon the quantitative findings. Specifically, quantitative data is collected first as it provides an over view of the research problem at hand and provides more robust analysis and qualitative data is there to refine and explain the general overview of the research problem (Creswell, 2012). Through the explanatory sequential design, quantitative and qualitative findings were integrated in the interpretation stage to provide a comprehensive understanding of the online risks, the cyber safety knowledge and attitudes of the university students. In the study the aim was to use data from expert reviews to expand on the findings from online questionnaires in order to develop a cyber safety awareness framework for university students.

1.7.2 Population and sample

The population for this study was all first-year students at the University X and University Y. The study used stratified random sampling to collect data from students at the selected universities in Eastern Cape, South Africa. The total population of first-year university students was 4308. An online sample size calculator (Survey Monkey sample size calculator) was used to determine the sample used in the study. Assuming that the population of the students followed a normal distribution at 95% confidence intervals producing a 5% margin of error, the estimated sample size was rounded up to 450 students to collect more data and ensure variability in the responses. Experts used to review the initial and final framework for cyber safety awareness were selected using expert sampling. Expert sampling implied that a non-probability selection of the respondents was made. Since the study was using a mixed method the selection of experts to be used for expert review was guided by Guest et al.,

(2006). Guest et al., (2006) indicated that sample size for purposive sampling is determined by the saturation concept which means that no new information or data was collected when the sample size was increased. There is no one size fits all on the sample size for qualitative studies but generally a sample size as reaching saturation between 6 and 12 and a maximum number of 30 (Guest et al., 2006). In this study, the experts were selected due to their knowledge of cyber safety. Six people were selected using expert sampling as no new data was being collected by increasing more experts. Thus, saturation was achieved when the sixth expert was selected.

1.7.3 Data collection

This subsection dealt with data collection methods, which ensured that adequate data was collected from the students, and the study relied mainly on primary and secondary data sources.

1.7.4.1 Secondary data

For the study, secondary data was collected from sources from peer-reviewed journals, textbooks and reports dealing with cyber safety awareness. Thus, in theory, secondary data was consulted to guide the study and answer the research questions under the literature review. Secondary data was also analysed through the use of content analysis for the most important factors which are related to the development of a cyber safety awareness framework for first year university students. The elements identified through content analysis were then used in the creation of critical success factors the development of a cyber safety awareness framework for first year university students as presented in Chapter 7 for this study.

1.7.4.2 Primary data

Data for this study is collected in online questionnaires due to the Covid-19 pandemic, where there is reduced face-to-face contact. Thus, the research collected data using online platforms like SurveyMonkey. The student's primary data focused on the risks they confronted when using the internet, their level of cyber safety knowledge, and the difficulties they encountered because of their different levels of cyber awareness. Online surveys were used to compile all of this information. Online questionnaires were also used to gather information from the students about the online risks, the level of cyber safety awareness among them, the

challenges they face in cyber safety awareness, and the solutions to those challenges. Data collected using online questionnaire was used for collecting the views of the students on their online presence, frequency and their cyber safety awareness. Data collected using questionnaires was used for testing of hypothesis formulated in Figure 1.1. The framework in chapter 1 was used to show the relationships between the independent and dependent variables. The dependent variables and the independent variables were used for hypothesis testing in Chapter 6. Data collected was also used to validate the views of the expert panel in the development of the cyber safety awareness framework.

Additionally, primary data also came from expert reviews. The researcher developed the initial framework for cyber safety awareness and was given to experts for review. The feedback from the experts led to the development of the final cyber safety framework. The experts also reviewed identifying critical success factors for developing a cyber safety framework. After two feedback cycles, the researcher developed a final version of the critical success factors. Overall, the role of the experts was to give feedback on developing the cyber safety framework and critical success factors. Data from the expert panel was used to firstly review and identify the critical success factors to be used in the development of the cyber safety framework. The expert panels were used to review the developed framework which was developed from Figure 4.3. With the modifications done on the critical success factors and the Figure 4.3 led to the framework presented in Figure 7.2.

1.7.4.3 Online questionnaire

A questionnaire is defined as a tool used in the collection of data. The participants can easily understand, infer, and fill in, which raises the answers the researcher gets from the study (Stockemer, 2019). Stockemer (2019) defines a questionnaire as an instrument comprised of respondents' questions. The study used an online questionnaire on cyber safety awareness to meet the current research demands. Specifically, the questionnaire collected data from randomly selected first-year students in the two selected universities. The researcher used a Survey Monkey online questionnaire of interactive forms to collect data. Respondents received an email requesting them to take part in the study. This survey was affordable as the results were instantly recorded in an online database, and modifications were made to the questionnaire when necessary.

Questionnaires are usually regarded as a research tool that generates findings that can be generalized to bigger samples (Harris & Brown, 2010). In this study, this implied that the online questionnaire results were generalized to the other students in the Eastern Cape. The online questionnaire had closed and open questions that were simple for the students to fill in during data collection (Phelas et al., 2011). The questionnaire collected Lickert-scaled data which is not easily collected using an interview guide. The level of cyber safety awareness among first year students in Eastern Cape was collected using a 4-point Likert scale with the following scales to measure the perceptions of the participants: "Strongly Agree" =1, "Agree" =2, "Disagree" =3, and "Strongly disagree" =4. In the questionnaire where the questions had a negative implication they were reverse coded implying that "Strongly disagree" =1, "Disagree" =2, "Agree" =3, and "Strongly agree" =4. The questionnaire was divided into five sections. Section A, covered students' profiles, including gender, age, frequency of online activity, and cyber safety involvement. Section B covered the online risks faced by first-year students in the Eastern Cape, and Section C covered the knowledge about cyber safety aspects among first year students in the Eastern Cape. Section D dealt with the cyber safety attitudes of the students and how this affected their cyber safety awareness. Section E looked at the measures used to deal with the challenges faced by university students when online.

Before using the online questionnaires to collect data, it was pretested. According to Phelas et al. (2011), pilot testing involves selecting a small number of participants to conduct trials of research instruments before the actual study is done. The piloting of instruments helped to identify problem questions and determine the time required to carry out the study. However, people used in the pilot study were not to be used in the actual study to reduce bias through prior knowledge of the study through piloting. The questionnaires were tested on a sample of none first year. Through the pilot survey, there was a refinement of the questionnaire questions. Problem questions were modified, so respondents had less difficulty understanding and answering the questions during the survey.

The research instruments had subsections based on the research scales presented in Table 1.1. From the literature, the researcher found several thresholds the scale items reached and were reliable and consistent. In the actual study, any variables below the set alpha =0.70 will be dropped from further analysis as they would bring unreliable results into the study.

Table 1.1.1: Reliability of scale items

Research scales	Alpha Cronbach	Source
Online risk	0.78	(Alzubaidi, 2021)
Cyber security attitude	0.713	(Chandarman & van Niekerk, 2017)
Cyber safety knowledge	0.791	(Matyokurehwa et al., 2020)
Cyber security awareness	0.90	(Muhirwe & White, 2016)

1.7.4.4 Expert reviews

Expert reviews are a research method that involves asking subject matter experts to evaluate a product, service, or idea based on their professional knowledge and expertise. The experts may be asked to evaluate a product or service based on specific criteria or standards, such as usability, functionality, or safety. The evaluation may be conducted through a structured questionnaire or interview. Specifically for this study, the experts were asked to review the critical success factors for cyber safety awareness and also to review the proposed cyber security framework. Since the research was carried out during the time of the Covid pandemic, phone interviews were used to collect data from the experts. In the case the experts had extensive knowledge about cyber safety awareness issues for first year university students.

1.7.5 Data analysis

To evaluate the reliability of the questionnaire instrument, Cronbach's alpha was utilized. The Chi-square test was used to examine the link between online frequency, online behaviour, cyber safety attitude, cyber safety knowledge, and cyber safety awareness. If $p < 0.05$, significant differences were found. The important success elements and the suggested framework for cyber safety for university students were determined through expert reviews. The online questionnaire needed to be tested to see if it could yield the same research results when utilized by researchers in different regions of the world and over different time scales because the study was quantitative. The Cronbach's alpha test will assess the instrument's reliability. The study measured the internal consistency of the online questionnaire using Cronbach's alpha test. Table 1.1, based on Cronbach's test, credible item scales were expected to have an alpha threshold over 0.70. Data from expert reviews was interpreted and synthesized the information provided by the experts to draw meaningful conclusions about the cyber safety framework. Thematic analysis was used to identify the themes (main factors) which were stated to be critical to cyber safety awareness. The feedback from expert reviews

was validated based on theories and literature reviewed in Chapters 2, 3, and 4. The input from the experts was checked to see if it was aligned with the variables aligned with the study's objectives, for example, cyber safety attitude, online risks and cyber safety awareness. If the reviewers' feedback were not in line with the objectives, the feedback was disregarded as it was irrelevant in determining the critical success factors.

1.8 Delimitation of the study

Regarding location, the survey was conducted among first-year students at University X and the University Y in the Eastern Cape. The study, therefore, examined first-year university students' understanding of cyber safety. As a result, the study's theoretical framework was informed by the theory of planned behaviour (TPB) and the social learning theory to identify the online hazards that first-year university students face and the extent of their cyber safety knowledge. The study concentrated on the degree of cyber safety awareness instead of the factors that led to the various degrees of cyber safety awareness. The study used first-year university students to determine the degree of high school pupils' understanding of cyber safety.

1.9 Ethical considerations

Ethics are the moral considerations that distinguish between good and bad (Bhattacherjee, 2012). Ethics are necessary for research to guard against manipulation by people or organisations to advance their agenda at the expense of the research subjects, which falls against the expectation of scientific conduct. The researcher made sure that the study complied with the ethical principles of the University Y's Research Ethics Council. This meant that the researcher's application for an ethical clearance must be cleared before the researcher began data collection. The University Y's Research Ethics Council approved the study with the following certificate reference number: PID011SMAK01. The permission to carry out research is attached as Appendix 2, and the ethical clearance is attached as Appendix 3. Permission was also granted to collect data from University X's students. The participant's agreement to engage in the study was explained on the top portion of the online questionnaire, which also included the purpose of the study. Confidentiality and anonymity were assured, and the researcher clarified that the study was academic. The researcher ensured that the research was anonymous by ensuring that there was no collection of personal information from the students. The students were informed of their right to withdraw at any

point during the data collection process without any consequences. The collected data was stored separately from the data used for analysis, and access was restricted to the researcher and the supervisors when needed.

1.10 Outline of chapters

This study consists of eight chapters, as follows:

- *Chapter 1* of the study presents the problem statement, aims, research questions, and hypotheses. Along with a brief assessment of the literature and research technique, the chapter also discusses the significance of the study.

- *Chapter 2* of the study highlights the transition for students from high school to postsecondary education. A theoretical framework adopted in support of the study is also discussed in this chapter, along with ways in which theories that informed the study were put into practice.

- *Chapter 3* presents the impact of cyber knowledge and attitude on cyber safety awareness.

- *Chapter 4* explores the requirements of the cyber safety awareness framework. This includes discussing the NIST framework and initiatives being made worldwide to raise people's understanding of cyber safety.

- *Chapter 5* covers the research methodology adopted to carry out the study from the beginning to the end. This includes the research paradigm, study design, data-collecting tools, and analytic techniques.

- *Chapter 6* presents the research findings for the study. The findings have collaborated with previously published research on cyber safety awareness.

- *Chapter 7* presents a framework for educating university students about cyber safety. The important success elements and the suggested models were improved through expert assessments.

- *Chapter 8* of the study covers the overall summary and conclusion. The areas for further study are also presented in this chapter.

1.11 Summary

The chapter provided an overview of the research's primary components, including the first-year students understanding of cyber safety in the context of a developing nation using South Africa as a case study. The Covid-19 outbreak was also examined in the chapter, concluding

that students were now more vulnerable to online dangers. The problem statement that the study aimed to address was also covered in this chapter. No high school or university curriculum in South Africa addresses pupils not pursuing computer science degrees. This meant that the switch to blended learning further increased the vulnerability of the students when engaged in online activities. In the chapter, there was coverage of the research objectives and questions that the study intended to answer. The chapter also briefly reviewed the theories which guided the study, namely the Theory of Planned Behaviour and the Social Learning Theory. The chapter also outlined the research hypotheses which the research intended to test.

The study's main aim was to develop a cyber safety framework that can be used in South African schools and universities to reduce the vulnerability of students when online. The chapter had to identify the context that led to the framework development for university students. By answering the study's objectives, the researcher made sure that there was a generation of answers from the students, which were key in developing the critical success factors and the cyber safety awareness framework.

The next chapter covers the context and theoretical background of the study. The chapter reviews the literature on the transition from high school to university. In the chapter, there is a review of the online risks that are faced due to the presence or absence of knowledge on cyber safety. The chapter covers the development of the Covid-19 pandemic and how this changed the way of learning globally and the online risks the students faced.

CHAPTER 2

CONTEXT AND THEORETICAL BACKGROUND

2.1 Introduction

The previous chapter covered the study's introduction, which put the study into context on the current state of affairs in terms of cyber safety and awareness, especially due to the COVID-19 pandemic. Specifically, the chapter addresses research question which was framed as follows: What is the association between online time and the hazards faced by first year students at a selected university in Eastern Cape? The chapter also addressed the secondary research objective which sought to determine the association between online time and the hazards faced by first year students at a selected university in Eastern Cape. This made universities switch to online learning, which exposed the students to more online risks without training on online learning. The research problem for the study is that the world has been affected by the Covid-19 pandemic, which has resulted in a shift from traditional to online and blended learning. All these changes have been done without much training for university teachers and students. The shift to online learning has increased cyber-crimes, such as phishing, by 400%. With this unprecedented increase in online crime, there is a need to look at the level of cyber safety awareness among university students in South Africa to develop a cyber safety awareness framework customised to the socio-economic stratification of the country.

This chapter reviews the literature on cyber safety awareness based on the transition from high school students to university level from a global perspective to the South African perspective. The chapter looked at how the theory of planned behaviour and the social learning theory was related to the context of the study. The chapter looked at the development of Covid-19 in China, how it spread to the rest of the world, and the different measures used to reduce its spread. The spread of Covid-19 meant that the students shifted to online, blended learning, which meant more exposure to online risks. The chapter reviewed the literature on the different ways which have been developed to reduce the effect of online risks faced by university students.

2.2 The transition from high school to tertiary education

The Internet creates a borderless world that exposes users to several threats. These threats happen everywhere, regardless of space, such as schools or workplaces (Asanan et al., 2017). A study by Kritzinger et al. (2017) revealed that children aged 7 to 16 spend about three hours online daily, but this figure rises to almost five hours for children between the ages of 15 to 16. As children spend more time online, about 9-25% are likely to become victims of cyberbullying. Many students are exposed to ICT devices at school, including mobile phones, tablets, and computer laboratories. ICT use in schools is becoming the standard. All stakeholders must be included in discussions about ICT and cyber safety, especially schools that offer or have access to ICT equipment for use in the classroom. All internet users of all ages are exposed to various risks depending on the time spent on the internet (Quayyum et al., 2021). Students spend time online for educational or entertainment reasons, but there are associated risks that students face simultaneously. Conversely, school students might easily become victims of cyber hazards and assaults since cyberspace is an uncontrolled and dangerous platform (Smit, 2015). However, age differences affect users' ability to separate threats from opportunities.

There are global variations in the age ranges for students to be in high school due to the differences in educational systems. This study adopted the 12-18 age range for adolescents used in the review by Quayyum et al. (2021). For adolescents, the main challenge has been exposure to appropriate content, such as internet pornography which affects attitudes, social development and brain development. The impact of cybercrime on school goers can be in the form of depression, digital avoidance, embarrassment, poor grades and dropping out of school (Kritzinger et al., 2017). It is, therefore, vital to ensure that students are educated accordingly on the matter. However, this study needs to be carried out to ascertain the degree of awareness of cyber safety in a particular context of South Africa because children's degrees of awareness of cyber safety vary from nation to country (Yilmaz et al., 2017). Cybersecurity education is already part of the curricula in certain industrialized nations. To safeguard its citizens, the United Kingdom (UK) government chose to teach cyber security to students from aged 11 years old to 14 years (Kritzinger, 2017). Several cyber safety efforts targeting demographics, including kids, teens, teachers, and parents, have been undertaken in industrialized nations. For instance, school curricula for kindergarten through grade 12 in the

USA now include computer security and internet safety training programs (de Barros and Lazarek, 2018).

Many high schools in the Eastern Cape and other provinces in South Africa have introduced e-learning in their learning curriculum (Kritzinger, 2017). Awareness of cyber safety is still at a minimal level (de Barros & Lazarek, 2018). The cyber risks facing children need to be understood by society, including parents and teachers (Asanan et al., 2017). Theoretically, the lack of cyber awareness of students implies that they are exposed to threats such as cyberbullying, pornography, loss of passwords, misleading information, and personal and financial data loss (Asanan et al., 2017). High schools in South Africa lack extracurricular programs or curricula for teaching cyber safety, putting young pupils at risk since they might not be aware of the risks linked with the internet (von Solms and von Solms, 2014; Waldock et al., 2022). In South Africa, the South African Cyber Security Academic Alliance (SACSAA) (www.cyber aware.org.za/) was established in June 2011. The SACSAA's primary objective is "to advocate for the effective dissemination of cyber security awareness throughout South Africa and to all demographic groups." A cyber safety awareness effort was also designed to help online users understand cyber security and know how to secure their information and themselves. The elderly, adults, and children are the key targets of the cyber safety awareness (de Barros & Lazarek, 2018). One of the cyber safety school programs is the UNISA My Cyber Safety Pledge. It is a poster designed to inform students about cyber bullying and urge them to sign the cyber safety pledge by providing guidelines for safe online conduct (de Barros & Lazarek, 2018). However, it has to be investigated how South African schools have reacted to the creation of the SACSAA in terms of raising awareness of cyber safety (Waldock et al.,2022).

More recently, the NCPF (Department of Telecommunications & Postal Services) mandated the development of South Africa's Cyber Security Hub. It disseminates information about security awareness through recommendations, posters, and campaigns. Since no target age category is mentioned, the intended audience is still unknown. Digital footprint, online privacy, dangers and hazards, cyberbullying, virus protection, password management, inappropriate material, and cyber scams are some of the subjects discussed. Along with teacher resources and student workbooks that may be utilized in the classroom, the Cyber Security Hub also offers workbooks for students. These workbooks specifically focus on online safety. These resources are extracurricular for teachers to include as they see fit into

their courses because this is not a part of the South African national curriculum. The Film and Publications Board (FPB) of South Africa also conducts awareness programs in schools; however, neither cyber security nor internet safety is included (Waldock et al., 2022).

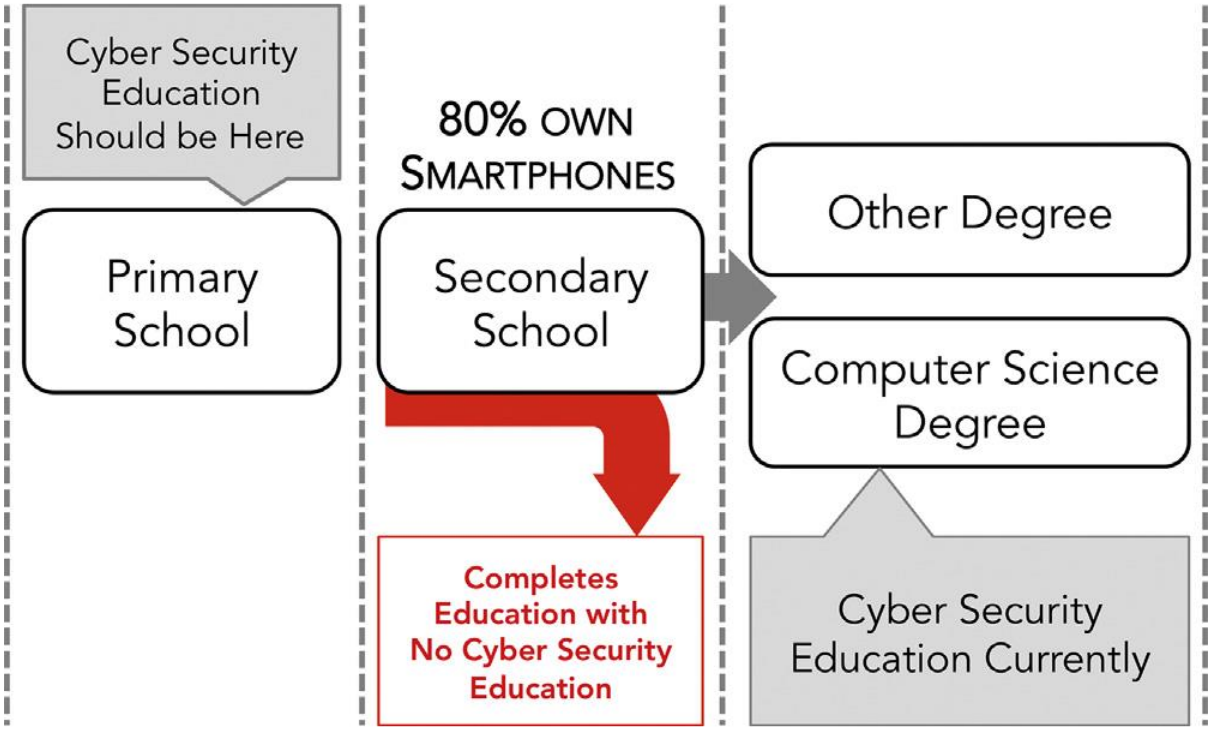


Figure 2.1: The anticipated South African security education approach (Source Venter et al., 2019).

Figure 2.1 shows the anticipated trajectory for the transition from high school to university. There is a gap in the provision of cyber security education, where in the university, it is taught only in computer science degrees (Venter et al., 2019). This worsens the gap between computer science degrees and non-computer science degrees. This means that most of the students that are not doing computer science degrees are vulnerable. Currently, cyber security education is provided (in universities), but it has to be provided in elementary schools (Figure 2.1). In this case, it has been determined that there is a need for improvement in the delivery of pre-university cybersecurity education. South Africa has a silo-based strategy since there are initiatives, politics, and legislation about cyber safety education. Still, each has a silo-based strategy and does not communicate with (connect to) one other (Waldock et al., 2022).

African nations are more susceptible to cyber-attacks due to the rapidly expanding internet availability (Grobler & Dlamini, 2012). However, several nations, such as Rwanda and Mauritius, have begun addressing cyber safety among students (Cole et al., 2008; Dlamini et

al., 2011). Most African nations, including South Africa, Uganda, Sudan, Egypt, Morocco, and Kenya, do not yet have policies to guarantee that school children are properly informed about cyber safety (von Solms & von Solms, 2014). According to Grobler and Dlamini (2012), Africa has a high proportion of computer illiteracy and poor laws, which has led to South Africa ranking third among nations with a high rate of cybercrime (Symantec Corporation, 2013).

African nations, in particular, are characterized by a lack of information, competence, and understanding of cyber safety, making it more difficult to design and implement cyber safety programs than in developed nations (von Solms and von Solms, 2014).

2.3 Application of theories to the study

The Theory of Planned Behaviour (TPB) was used to determine an individual's online behaviour, decisions and the security measures adopted. Additional factors such as knowledge and personal experiences were added to the TPB, as these factors directly impacted a person's attitude. The level of cyber security awareness can influence the attitude of the user. Awareness of threats in the context of information, communication and technology (ICT) is regarded as one of the drivers of attitude (Vafaei-Zadeh et al., 2019). The theory will examine the attitudes and norms of students engaged in online learning due to the Covid-19 pandemic. TPB suggests that attitudes and norms the person thinks are subjective and affect the individual's behavioural intent, eventually affecting actual behaviour. An individual's attitude towards a specific behaviour will be based on a negative or positive appraisal of the individual's conduct. Subjective norms will be influenced by the forces around the individual such that there is engagement or non-engagement of a particular behaviour (Burns & Roberts, 2013). A person's attitude towards a particular behaviour is related to the individual's perception towards a certain element. In this case, an individual's attitude will affect the person's behaviour. In the context of cyber security awareness, if a person is aware of the dangers of not protecting their computer, it will lead to the quest to have computer protection through an anti-virus, for example. Installation of virus protection or spy software on computers is not enough as this cannot save the user from hackers or having information stolen (Hunt, 2016). This level of awareness leads the user to secure the computer, which implies that the user will develop a positive attitude towards protecting the computer.

Research has indicated that attitude towards cyber security positively relates to the person's intention to behave (Vafaei-Zadeh et al., 2019). There is a need for a change in the way of thinking to recognise that there is a need for other security measures which can increase protection from threats rather than only having virus protection. The theory was relevant to this study as there is a need to determine online risks facing first-year students at selected universities in Eastern Cape. The research intended to develop measures to prepare online risk-specific awareness rather than generalizing them. The TPB is interested in the study to determine the level of cyber safety awareness among first year students in the Eastern Cape. This was based on their attitudes towards the risky behaviour that they exhibit when they are online. Thus, the study's findings can be used as a launchpad for schools and policymakers when creating cyber safety awareness strategies. The theory was relevant in this study as it can predict the student's online behaviour. There was a need to look at the theoretical relationships between the TPB variables and how these affect cyber safety awareness among young university students such that there was a determination of the similarity or dissimilarity of the research findings (Alotaibi & Mukred, 2022). The researcher recommended the cyber safety awareness measures for the first-year students at University X and University Y in the Eastern Cape from the online behaviour.

Akers put forward the Social Learning Theory (SLT) based on the behavioural learning approach. This concept relates to the proposed study because first-year student associations affect the individual's online behaviour and the associated challenges. The other concept of the SLT is the attitude, which implies how a person perceives good and bad (Gabra et al., 2020). Specifically, the study refers to how an individual views online behaviour and the awareness towards cyber safety for first year students at selected universities in Eastern Cape. The other component of the SLT is differential reinforcement, which means the gains and losses associated with some behaviour. Imitation is another concept of the SLT, which implies that there is observation of some behaviour and copying the individual's same behaviour. In this study the individual can imitate online behaviour and also the cyber safety measures which can be copied or not copied. Overall, the SLT will be used in this study to explain the variability in terms of online behaviour and level of cyber safety awareness.

2.4 The Covid-19 pandemic and increased online risks for users

The World Health Organization (WHO) declared the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) that caused the 2019 coronavirus illness (COVID-19) a pandemic on the 11th of March 2020. Wuhan, China, was the first place where SARS-CoV-2 was discovered (Ghazawy et al., 2021; Gumede and Badriparsa, 2022). The droplets produced by a person's coughing, sneezing, and exhaling are the major ways in which the virus that causes COVID-19 is spread (Chigada & Madzinga, 2021). Because these droplets are too heavy to hang in the air, they can also settle on surfaces. This increases the risk of infection and transmission when people come into contact with them. The typical Covid-19 infection symptoms include respiratory issues, fever, coughing, and shortness of breath (Mpungose, 2020). The United States (9.4 million cases), India (8.2 million cases), Brazil (5.5 million cases), and Russia (5.5 million cases) were among the nations with high COVID-19 infection rates (1.7 million).

Covid-19 created mass panic around the globe (Olaniran & Uleanya, 2021). Due to the nature of spreading through contact with the infected person, Covid-19 spread to all parts of the world. The Covid-19 pandemic led to millions of infections and death across the globe. Due to the millions of infections, several measures were adopted. These measures included banning international flights, social distancing (measuring 1m from the next person), sanitising hands frequently, wearing face masks, working from home, banning social gatherings such as funerals, weddings, churches, and schools were closed, and different countries imposed lockdowns and curfews (Laher et al., 2021; Tick et al., 2021). The closure of educational institutions led to a change from in-person to online learning, and educational systems were not exempt from this trend. For example, in April 2020, over 3.4 billion people, almost 43% of the global population, were under lockdown in over 80 nations and territories across the globe (Marinoni et al., 2020).

To curb the spread of Covid-19, specifically in South Africa, a national disaster was declared on the 15th of March 2020. This meant a need to develop new policies to deal with the pandemic. There was an abrupt shutdown of schools and other institutions of higher learning, and classes resumed using the online mode of teaching and learning (Ntombela, 2022). In the South African context, the President requested that, as a preventative step, all universities close on the 18th of March 2020 and find a means to give courses online (Mpungose, 2020).

Between July and September 2020, there was a global decrease in COVID-19 infections, which led many economies to loosen their strict controls and return to their normal economic activity by focusing on social isolation, mask usage, and other health-related behaviours. South Africa's level of national lockdown was lowered from level five (complete closure of the country except for essential services) to level one on the 1st of October 2020, allowing people and companies to go on regular business while monitoring and adhering to healthcare laws. People who lived, studied, or worked in South Africa experienced uncertainty and isolation during the first quarter of the COVID-19 pandemic, sometimes known as the "hard lockdown" phase or Levels 5 and 4 of the COVID-19 pandemic lockdown levels (du Plessis et al., 2022).

2.5 Covid-19 pandemic and the shift to online education in South Africa

As described in the previous section, Covid-19 unexpectedly spread worldwide, affecting several sectors of the economy, with higher education not spared (Shakeel et al., 2022). Within the South African context, online education was introduced. There was no sudden stopping in learning which meant that universities had to avoid the challenges of spreading Covid-19, such as keeping social distance. As a remedy to avoid these challenges, face-to-face teaching had to be cancelled (Gumede & Badriparsa, 2022). Institutions in South Africa have used conventional teaching and learning techniques, like most educational institutions worldwide. The traditional means of learning meant that the students and the lecturers would be engaged in face-to-face teaching and physical contact with the students. However, the Covid-19 epidemic has caused a change in how education is delivered globally, and South Africa has not been exempted (Mpungose, 2020).

Institutions have shifted to online learning, while some have resorted to blended learning, including online (e-learning) and physical classes (Figure 2.2). From Figure 2.2, it can be noted that there was an extreme and sudden shift from physical to online learning in a short period. In this case, e-learning involves learning over the internet and is also called online learning, distance education and web-based education (Le Grange, 2021; Mpungose, 2020). With all the names, online learning does not include face-to-face teaching but learning from a distance.

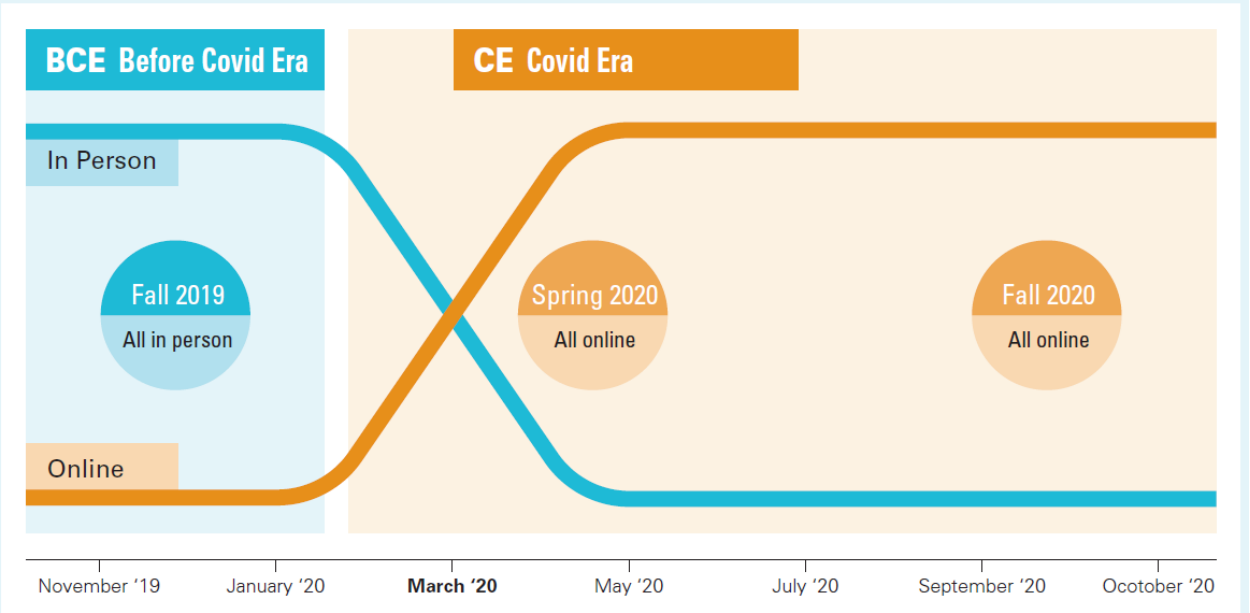


Figure 2.2: Shift from face to face teaching to online teaching at the peak of the Covid 19 pandemic (Source: Salami, 2021)

Due to the Covid-19 epidemic and the consequent closing of schools and institutions, internet traffic increased by 50% (UNICEF, 2020). Using blended or wholly online means of learning means that the students and the teachers have more time online. This meant an increase in the probability of the students being exposed to challenges associated with over-access to online technologies. Most academic institutions have been worried about accessibility, cost, flexibility, learning methodology, lifelong learning, and policy towards online learning as the amount of time until the epidemic eased grew (Dhawan, 2020).

Higher education institutions were unprepared for the sudden shift from in-person to online learning that the COVID-19 epidemic brought about (Mncedisi et al., 2021). 26 public higher education institutions (11 general academic universities, nine comprehensive universities, and six technical universities) are located throughout South Africa's nine provinces (Olaniran & Uleanya, 2021; Patrick et al., 2021). As a reaction to COVID-19, universities around South Africa have positioned learning management systems (LMS) as essential to distance teaching and learning (Dlamini & Ndzinisa, 2020). For web seminars (webinars), conference calls, and videos to foster interpersonal relationships, some frequently utilized platforms include Zoom, Microsoft Teams, and Skype (Patrick et al., 2021). For example, the University of KwaZulu Natal (UKZN) started using learning management systems such as Moodle in 2016, which was made compulsory for first-year students in 2016 and fourth-year students in 2019

(Mpungose, 2020). However, the adoption of online teaching impacted both lecturers and students as no training was offered for using Moodle (Hedding et al., 2020; Tick et al., 2021). South Africans entered the COVID-19 lockdown in various socioeconomic situations, so lecturers should be aware of the pre-existing cultural categorization (Gumede & Badriparsa, 2022). To embrace online learning and change with the times, universities had to invest significantly in digital technology. From the beginning of the nationwide lockdown, some students had access to online learning tools, but many relied on the government for free cell phones, tablets, or computers and data (Laher et al., 2021). A few educational websites have also been made data-free for students. However, the major online platform (Blackboard and its multiple platforms) is not available for free access because it is not housed in South Africa (Hedding et al., 2020). However, differences in the student's socioeconomic statuses could create inequality.

Universities reopened for the academic year on digital online platforms on the 20th of April 2020, supported by agreements with telecom firms to give free bandwidth to all students starting on that day and zero-rated websites to enable remote teaching and online learning (Pillay et al., 2021). Several schools even acquired computers to loan students to guarantee that students could access online learning platforms. The lack of preparation and adequate access to digital learning tools for students has prevented them from reaching their learning objectives (Dlamini & Ndzinisa, 2020). It can be noted that the considerations of the universities and the South African government have been the provision of digital technologies to the students and university staff, with less attention being given to the cyber safety of the students. However, some students lack digital literacy, a critical skill for navigating different digital technologies used by universities (Dlamini & Ndzinisa, 2020; Mpungose, 2020). Several research groups have established communication tools like Zoom, WhatsApp, and Google Groups to stay in touch, organize research, and uphold group spirit and a research culture while working remotely (Hedding et al., 2020).

2.6 Covid-19 pandemic, cyber threats and cyber security awareness

Through a raft of measures adopted by several countries, universities were commonly closed, which meant that students accessed materials over the internet. This was due to the availability of modern technology, such as hardware in the form of laptops, cell phones, and tablets, and software resources such as learning management systems, software applications

and social media sites (Mpungose, 2020). The combination of software and hardware meant that students could access content and information from anywhere and anytime during the pandemic (Mpungose, 2020). In a study on first-year students on the use of social media in South Africa, it was found that students became interactive when using the platforms they were familiar with compared to the learning management systems offered by the university.

An additional severe hazard to a technologically advanced civilization brought on by the Covid-19 epidemic was an increase in targeted and indiscriminate cyber-attacks (Lallie et al., 2021). The increase in cyber-related attacks on the educational front can be attributed to a lack of adequate security resources to push for online-related learning. However, during the Covid-19 epidemic, the focus has been on implementing online education, paying less attention to the online danger students would face when taking online courses. With the pandemic shifting towards more online learning, there is a need to determine the cyber safety levels to provide digital safety for students outside the school premises (Siyam & Hussain, 2021). The radical shift from physical learning to online teaching has not been met with equal treatment regarding cyber security, especially in the developing world (Salami, 2021). The need to look at the safety of the students emanates from the view that the changes in technology bring about changes in attitude, behaviour and perception. The shift to online technology was introduced due to the Covid-19 pandemic.

Online learning meant students used social media platforms to connect with their peers, teachers, or lecturers. As a result of the students' increased exposure to various cyber crimes due to using social media for teaching and learning, there is a need to reconsider student knowledge and safety about cyber crimes. For example, in the United Kingdom alone, the switch to online teaching and online has led to 400% during the pandemic, and the common attacks have been emailing and Phishing (Marinoni et al., 2020). As hundreds of schools and institutions have extended their online presence, there has been an upsurge in cyber incidents. These cases vary from innocuous phishing attacks directed at students and professors to trivial intrusions into Zoom conferences to more significant data thefts and ransomware assaults (Salami, 2021). The cyber attacks come from attempting to gain unauthorised access by pretending to be authentic in emails. If an attack becomes successful, there is a compromise in the integrity and confidentiality of the information stored on the online gadget. In 2020, Educational institutions spent over $2.5 million on recovering downtime, repairs, and lost opportunities due to cyber attacks.

Another example is that educational organizations suffered eight attacks on their Domain Name System (DNS) in 2020, and each attack cost over $850,000. There is no size fit for the measures that can deal with students' daily learning of cyber crimes. The goal is to keep students informed about the dangers they face when participating in online learning during the Covid-19 epidemic. Students encounter difficulties with phishing, data and identity theft, malware infection (such as viruses), cybersex predation, exposure to inappropriate information, and cyberbullying (Siyam & Hussain, 2021). In the first three months of 2020, phishing email assaults connected to COVID-19 increased by 600% in South Africa, according to KnowBe4, a security awareness training company located in South Africa (Salami, 2021). Higher education institutions manage complicated networks that are accessible to huge numbers of students and faculty members, making them more vulnerable than other types of organizations. They also frequently rely on platforms from third-party suppliers, increasing their exposure (Salami, 2021). Due to a lack of knowledge about cyber threats and a lack of funds to employ a cyber security company and migrate their databases to the cloud, these networks frequently run without effective protection. However, the school authorities need to deal with issues related to cyberbullying, although research by Safa and Von Solms (2016) indicated that the school authorities give less attention. However, since it has been about six years since the research was done, it needs to be looked at the measures schools have instituted against cyberbullying among students.

Due to the rising demand for working from home, most businesses are prone to security breaches because they have weak cybersecurity procedures and unsecured data. Campaigns to raise awareness of cyber security issues, instructional programs, preventative measures, and creating a cyber security culture would assist (Chigada & Madzinga, 2021). A cyber security architecture that includes a full suite of management tools, a thorough risk management strategy, and a security awareness program that covers everyone in the organization from top to bottom is required. However, providing awareness programs cannot be enough to deal with cybercrime and the associated threats. There is a need for frameworks which includes all stakeholders and a code of ethics to deal with unruly behaviour. More so, the framework needs to be supported by the necessary legislation which can be used for enforcement purposes. On the other hand, it's important to practice good online behaviour by confirming sources and following official announcements (Chigada & Madzinga, 2021).

2.7 Technologies and cyber safety

Cyber safety can be referred to as the safe and responsible use of Information and Communication Technologies (ICTs) (Zulkifli et al., 2020). The notion of cyber safety highlights the necessity for students to be aware of how their activities or those of others might have negative repercussions. Cyber safety emphasizes the measures that should be taken and what pupils should consider when using the Internet. Securing personal information and data, protecting digital identities, using technology safely and sustainably, and adhering to security protocols are all key components of online safety and fall under the category of cyber safety (Matyokurehwa et al., 2020). Understanding cyber safety among first-year students in the Eastern Cape must thus be ascertained.

The human element, typically the weakest link in cyber security, is the focus of the growing number of online criminals who commit an ever-widening range of cyber crimes (Chandarman & van Niekerk, 2017). Thus, there is no question about the necessity of cyber safety awareness efforts, which continue to be the first line of defence in educating young people about how to engage securely online. Because they are less conscious of online safety, students are more likely to be cyber attack victims. To safeguard people and systems, cyber safety awareness is a vital line of defence (Chandarman & van Niekerk, 2017). In addition to information, proper awareness and attitudes are crucial for fostering secure online behaviour.

Young children are at risk because schools lack extracurricular programs or curricula for teaching cyber safety, and they might not be aware of the risks linked with cyberspace (von Solms & von Solms, 2014). Aiming "to promote the effective dissemination of cyber security knowledge throughout South Africa to all demographic groups," the South African Cyber Security Academic Alliance (SACSAA) was established in 2011. As a result, the study contributes to the creation of a framework for cyber safety among the population of first-year students. Even though the cyber safety awareness project was done to increase the spread of knowledge and understanding of cyber safety awareness, the increase in the number of cyber-related challenges calls for this study to determine the shortcomings of cyber safety awareness for first year students. Its main aim is to target children, adults and the elderly (de Barros & Lazarek, 2018). One of the cyber safety school programs is the UNISA My Cyber Safety Pledge. Still, this study needs to determine how the pledge has affected students' cyber safety awareness in their first year of university life (de Barros & Lazarek, 2018). Although

some interventions already exist, there is a need to determine the experiences of first-year students in the Eastern Cape regarding cyber safety awareness.

2.8 South Africa and the Covid-19 pandemic

Globally, every country has been impacted by the COVID-19 pandemic, also known as the coronavirus disease. While several nations have passed the height of this unprecedented global epidemic, South Africa still sees its impacts. The virus's transmission has been slowed by several techniques, including wearing facemasks and avoiding social situations (Mukuna & Aloka, 2020). Public events, educational programs, and commercial activities must be cancelled to enforce these restrictions and encourage people to stay home. Higher education institutions were taken off guard by the sudden shift from in-person to online learning that the COVID-19 pandemic brought about (Mncedisi et al., 2021). Six universities of technology, nine comprehensive universities, and eleven general academic universities make up South Africa's 26 public higher education institutions, dispersed throughout the nation's nine provinces (Patrick et al., 2021). Universities had to find quick fixes to prevent disruptions to learning, provide the necessary technological infrastructure for online classes, equip academics with the skills necessary for conducting virtual instruction, and ensure that students had access to the required equipment and internet connectivity (Mncedisi et al., 2021). In South African schools, learning was interrupted due to the COVID-19 lockdown, and students and teachers in remote regions could not engage in online learning. In response to COVID-19, universities throughout South Africa have made learning management systems (LMS) a key component of distance learning (Dlamini & Ndzinisa, 2020). Web seminars (webinars), conference calls, and videos are some of the often-employed platforms, with Zoom, Microsoft Teams, and Skype among them (Patrick et al., 2021). Because South Africans had a variety of socioeconomic situations when they joined the COVID-19 lockdown, professors should be aware of the pre-existing cultural categorisation (Gumede & Badriparsa, 2022). To adopt online learning and keep up with the changes, universities have had to make large expenditures on digital technologies. While many students depended on the government for devices like cell phones, tablets, or computers, as well as free bandwidth, some could access online learning platforms right after the country was locked down (Laher et al., 2021). Universities started the academic year on digital online platforms on April 20, 2020, backed by agreements with telecom companies to provide free bandwidth to all students starting that day, as well as zero-rated websites to promote remote teaching and

online learning (Pillay et al., 2021). Several universities even went so far as to buy computers to loan to students to ensure that students could access online learning platforms. Students find completing their online learning objectives challenging due to a lack of preparation and restricted access to digital learning tools (Dlamini & Ndzinisa, 2020).

The educational system in South Africa (SA) has significantly changed to keep up with the speed of learning (Gumede & Badriparsa, 2022). Most South African educational institutions have abolished contact-based learning activities from their curricula due to the demand for social distance. Online learning was developed to guarantee that education will continue. It may be described as instruction delivered via a digital medium to foster learning. At South African universities, there are considerable challenges to lecturers' misconceptions about online learning platforms, lecturers' access to computer equipment and the related support and training requirements, and students' access to computing devices and data (Dlamini & Ndzinisa, 2020). The difficulties that would arise after the pupils were given access to digital tools are being ignored in this case. During the Covid-19 epidemic, there is less focus on students' internet safety and their understanding of the dangers to which they are exposed.

2.9 Online risks facing university students during the Covid-19 pandemic

Working from home exposes people to cyber threats since they connect over unreliable and open Internet connections (Chigada & Madzinga, 2021). Due to the Covid-19 epidemic, more kids were doing their schoolwork from home, which resulted in increased internet usage and online time spent, as well as more online threats. Some common threats were spam mail, malware, suspicious websites and domains, attacks from Distributed denial of service (DDoS) and social media messaging (Wang & Alexander, 2021). Youngsters are particularly fascinated by information and communication technologies (ICTs), such as the Internet and cell phones, since they meet some of their most important emotional and communicative demands (Gámez-Guadix et al., 2016). As they transition from a life focused on their parents to one where peer association predominates in forming their identities, students go through a period of increasing risk-taking and thrill-seeking (Knowles et al., 2014). Students seek approval and connection with their classmates. Still, their capacity to see beyond their actions' immediate repercussions and hazards vary depending on age, cognitive capacity, and psychosocial developmental stage (Knowles et al., 2014).

As described by Paluckait and Ardeckait-Matulaitien (2016), risky online behaviour can be summed up as dangerous online behaviours that pose a threat to the user. To put it another way, risky behaviour may be defined as the propensity to participate in actions that have the potential to be damaging and hazardous but may also result in a result that is positive and exciting at the moment of the action (De Gouveia, 2013). Risky behaviour may result from sensation-seeking behaviours (which rise in students), as these actions frequently give unexpected and strong stimulation that persons with increased sensation-seeking find delightful (De Gouveia, 2013).

According to Cabello-Hutt et al. (2017), 92% of today's youth use the Internet and other digital gadgets daily. 24% of them use the internet "nearly continuously," while 56% do so often each day. Only 12% reported going online once daily, and only 2-6% noted using it less than once a week. The risks associated with these teenagers' constant access to the Internet via a computer, smartphone, or tablet are numerous (Liau et al., 2006; Schilder et al., 2016). Adolescents' internet activities cannot be classified as good or detrimental since evaluations of an activity's value are based on its results rather than the activity itself. While there are many advantages to using the internet, there are also risks. Access to global information, educational resources, entertainment, social networking with friends, privacy for identity expression, content production, and civic or political involvement are just a few examples of online options. Online hazards might include unlawful information or activity, sexual assault, bullying, privacy breaches, defamatory material, and harmful software (Cabello-Hutt et al., 2017; Kritzinger, 2017).

Cyberbullying, sexting, communicating with strangers, sending embarrassing photos, sharing their location publicly, and the spread of risky pranks and games are just a few of the online risks that students may encounter when they are online (Beverley & Covey, 2018; Paluckait & Ardeckait-Matulaitien, 2016). Sexting is another form of online risk that a stranger can do, a friend and or an acquaintance, whereby sending or receiving sexual images, videos, and texts online. This is also classified as a form of sexual solicitation. Sexual solicitation usually leads to risky sexual behaviour online. Students that engage in online activities have the danger of being exposed to content risks, contact risks, economic risks, and privacy hazards (Al-Badi et al., 2016; Schilder et al., 2016). Contact dangers include exposure to pornography, difficult content, and sensual/violent/racist/hateful stuff (e.g. suicide, anorexia,

drugs, etc.). Students frequently look for improper information, discuss delicate subjects, read about, and see online postings on these themes.

Risks associated with contact include interactions with foreigners, internet abuse, and cyberbullying. The Internet may give teenagers access to much information but can also expose them to additional dangers and hazards. They could come across dangerous people and sensitive data and become the focus of online harassment and bullying. Teenagers are more susceptible to contact risk when communicating with strangers, disclosing private information or photographs, and participating in questionable actions (Al-Badi et al., 2016; Schilder et al., 2016). Advertising and commercial usage, illicit downloading, and gambling are commercial dangers. For copyright concerns, it is forbidden to download music from the Internet into consumers' computers, and scholars consider unlawful online music downloading to constitute theft. Examples include spam and the misuse of personal information (Schilder et al., 2016). Privacy threats include personal information disclosure and publishing, invasions, hacking, and identity theft. Identity theft is like phishing, implying that personal information is shared through several web services or social networks. It isn't easy to control the personal information shared (Quayyum et al., 2021). The problem with identity theft is that the stolen personal information can be compromised, further worsened by the users' online misbehaviour or online attitude.

There is a propensity to share personal information online, especially on social media platforms. The potential of harassment, cyberbullying, privacy invasion and unwelcome sexual advances can all arise from sharing personal information and images. These two categories are also mentioned as the most systematic risks in the EU Kids Online report, which also lists chats with previously unidentified online contacts, cyberbullying, pornography, sexting, texting, websites with harmful user-generated content (hatred, support for anorexia, drug use, or suicide), data abuse, and excessive Internet use (Schilder et al., 2016). Table 2.1 summarises online risks and their sources and values, which online users can suffer. The risk is categorised as content risks in which the user receives inappropriate content; the other risk is contact risk, with risky communication with other people or peers (Staksrud & Livingstone, 2009). Conduct risk is risk in which the user contributes risky content.

Table 2.1: Summary a summary of online risks and their sources and values (Source: Alhejaili, 2013)

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct(child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

2.10 Summary

The chapter provided the context and the theoretical background of the study. It has been noted that there are differences between countries in terms of the level of cyber safety awareness given to children from up to the university level. Despite having a cyber security framework, South Africa was found without a curriculum that teaches cyber safety, especially at lower levels of learning. The chapter discussed how the Covid-19 pandemic spread from China to all parts of the world and there was a shift in how schooling at all levels was carried out. A new way of online learning was introduced without proper training for educators and students, and the lack of training was also met with increases in cyber-crimes across the

globe. The chapter explained the different types of cyber threats that the students faced. The chapter looked at how the theory of planned behaviour was used to explain the different forms of behaviour that need to be addressed to achieve cyber safety awareness. The chapter also discussed the view that the risk faced by the students can be due to online behaviour, which is acquired from members of society such as friends.

The problem of the study was the absence of a cyber safety framework for university students in South Africa. The chapter identified that the students spend more time online due to online and blended learning used by the universities, which increased their exposure to online risks. The risks identified were key inputs into the development of the cyber safety framework and the critical success factors needed for the development of the framework.

The next chapter focuses on cyber safety knowledge, attitude, and awareness. The chapter reviews the key concepts for the study: cyber safety knowledge, cyber safety attitude, and cyber safety awareness. The chapter also looks at how cyber safety knowledge and attitude affect the cyber safety awareness of university students, especially during the Covid-19 pandemic.

CHAPTER 3

CYBER SAFETY KNOWLEDGE, ATTITUDES AND AWARENESS

3.1 Introduction

The previous chapter outlined the context and theoretical background of the study. The chapter discussed students' transition from high school to university across countries of different socio-economic and political development. The chapter also dealt with the spread of the Covid-19 pandemic and how this changed the way of life and learning for university students. Increased online presence meant that the students were more likely to face cyber threats.

This chapter aimed to introduce central terms in the study, such as cyber safety, cyber safety knowledge, cyber safety attitude, and awareness. The chapter intended to answer the following research questions: How does cyber security knowledge affect cyber safety awareness among first-year students in the Eastern Cape? How does cyber security knowledge affect cyber safety awareness among first-year students in the Eastern Cape? Moreso, the chapter intended to also fulfil the objective that sought to determine the effect of cyber security knowledge on cyber safety awareness among first year students in Eastern Cape. The other objective intended to be fulfilled by the chapter was examining the effect of cyber security attitude on cyber safety awareness of first year students in Eastern Cape. The chapter also reviewed the literature on cyber awareness is becoming more and more important as data usage and internet usage rates rise. However, the rise in internet usage is not countered with an increase in cyber safety knowledge about the online risks and measures that can counter the threats faced. Knowledge about the different types of cyber threats is a starting point for developing a better attitude toward online measures to reduce the risk of online threats. However, knowing does not necessarily translate to improved cyber safety awareness.

The chapter explained the factors which come into play in the attitude towards cyber safety awareness. The chapter looked at the effect of cyber safety knowledge on cyber safety awareness. The chapter also discussed literature at a global scale about how cyber safety

attitudes affected the cyber safety awareness of university students. These factors were key inputs in developing the critical success factors and the elements of the cyber safety framework developed later in the study.

3.2 Introduction to cyber safety

According to Alqahteni (2022), users of digital technologies may be more in danger as they are more thoroughly incorporated into daily life. Cyber security must be considered against shifting technological trends, goods, and behaviours. Cyber safety, also known as online safety, internet safety, e-safety, and digital safety, is widely understood to be the responsible and safe use of Information and Communication Technologies (ICTs). Forrest-Lawrence and Collier (2014) point out that the topic of cyber safety encompasses a wide range of subjects, including online privacy (including the use of privacy settings); online etiquette (or netiquette); cyberbullying; sexting and sextortion (extortion involving digital sexual imagery and distribution); online sexual predation and grooming; and personal information security (e.g. keeping personal information such as images and identifying details safe); and digital footprints (sometimes referred to as online reputation); safe social networking; accessing inappropriate content; internet and device addiction; safety when gaming online; security tools and filtering software; digital fraud; hacking; online piracy; and plagiarism.

The idea of cyber safety highlights the necessity for students to be aware of how their activities or those of others might have negative repercussions. Cyber safety also focuses on the things that students should think about and take into account when using the Internet. Cyber safety includes protecting personal information, data, and digital identities, security measures, safe and sustainable technology usage, and other key components of Internet safety (Hatlevik & Tomte, 2014; Laher et al., 2021). Cyber safety extends beyond safeguarding children from online predators and stopping cyberbullying. Cyber safety includes minimizing exposure to risks such as internet and gadget addiction, fraud, identity theft, privacy breaches in credentialing, malware, phishing, and scams, as well as violent and sexually explicit content, games with weak security, and sextortion (extortion involving digital sexual imagery and distribution) (Hatlevik & Tomte, 2014; Laher et al., 2021). Thus, it is necessary to ascertain the attitudes and opinions of the pupils in Mthatha about the concept of cyber safety.

An increasing number of online criminals performing an ever-widening spectrum of cyber-crimes usually target the weakest link in cyber security that is the human factor. Since they remain the first line of defence in arming young people with the knowledge to engage securely online, the necessity of cyber safety awareness programs is thus undeniable. Due to their ignorance of cyber security, students are more likely to be victims of assaults online. An important line of defence in defence of people and systems is understanding cyber safety (Chandarman & van Niekerk, 2017; Wang & Alexander, 2021). To promote and secure online behaviour, the right awareness and attitudes are just as important as knowledge.

Although there are advantages to using the internet, some partially concealed hazards come with it. The objective of educators is for students' online experiences to be safe and fulfilling, and to achieve this goal; schools must make sure that kids are protected appropriately through instruction in safe Internet usage. Teachers are supposed to be accountable for their pupils' safety and the Internet-related lessons they teach. Yet, they might not fully comprehend their students' dangerous, harmful, or immoral online behaviours (Olaniran & Uleanya, 2021).

3.3 Cyber safety knowledge

In reality, people are increasingly relying on internet technology for daily work. The accessibility of such activities has enabled widespread engagement. However, awareness of the technologies already available and necessary for cyber threat defence is still lacking. Basic cyber security knowledge could not transfer into sufficient or suitable cyber security protection skills to reduce cyber risks and hazards (Vafaei-Zadeh et al., 2019; Zwilling et al., 2022). Increasing cyber security awareness through training programs that expose students to cyber security defence tools through theoretical lectures and simulations. These would emphasise the operational, use, and procedural elements of enhancing user comprehension and turning it into efficient cyber security mitigation behaviour. For instance, a well-liked training tool called "Phishing Simulator" was created as an effective training procedure to raise awareness of dubious e-mails from hackers. Such emails frequently contain harmful software, or "malware," which causes unauthorized data leaking. The simulator is also appropriate for instructors, providing access to useful security tools to reduce phishing emails and internet links and directing them to achieve the highest levels of defence against cyber security risks. Initiatives help people become more aware of and knowledgeable about cyber hazards. It has been predicted from Figure 3.1 that cyber knowledge and cyber safety

awareness have a linear connection. As a result, as one's degree of cyber knowledge increases, so does their awareness of cyber safety, which leads to actions that promote cyber protection. The cyber knowledge itself, however, might also result in cyber protective behaviour, as seen in Figure 3.1.

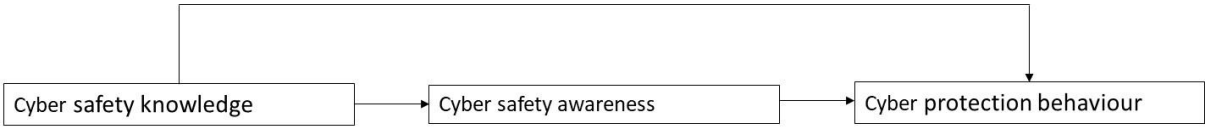


Figure 3.1 Conceptualised relationship between cyber safety knowledge and cyber awareness (Adapted from Zwilling et al., 2022)

Training is there to improve the cyber safety knowledge of internet users. For example, training on improved knowledge of phishing was evaluated. Training initiatives aim to increase users' understanding of and sensitivity to possible cybersecurity risks. Before and following cyber security training, they concentrated on knowledge of password protection and the capacity to safeguard computers. They emphasized the crucial function of cyber education and training, focusing on suitable security procedures to enhance regular online activity. Campaigns to raise awareness may help to curb online risk-taking. Students were encouraged to use complicated passwords because of their exposure to and experience with them in training programs. They proposed that offering security awareness training programs might significantly impact people's attitudes toward information security management. The training style should be decided by a combination of delivery techniques (such as text-based, game-based, and video-based). Courses on cyber security should be problem-centred and include case studies appropriate for the student's knowledge levels.

According to Zwilling et al. (2022), respondents with more computer science expertise had a stronger positive relationship with cyber security awareness. The majority of people do not, however, have the choice of specializing in computer science. According to planned behaviour, the intention is the greatest indicator of any planned conduct. Since risks to computer security are considered seriously, it is more probable that someone will be motivated to implement the necessary safeguards. However, factors like the degree of self-efficacy and controllability can impact behaviour. As a result, the belief that one influences circumstances owing to personal knowledge motivate one to take action.

3.4 Cyber safety attitude

An attitude toward internet safety may be described as a positive or negative set of assumptions about the topic and its problems (Okanlawon et al., 2015). The term "attitudes" in the context of cyber security refers to a person's point of view, which might affect their conduct online (Antunes et al., 2021). These attitudes, which may influence how a person chooses a certain event in their online activity, are the product of their learning experiences, social variables, and observation. In instances where they are substantially activated and when the actor recognizes a relationship between attitude and behaviour, attitudes have predictive value. Affective, cognitive, and behavioural components all makeup attitude. The gut sensations a person has concerning something or someone comprise the emotional component. An assessment based on attributes creates the cognitive component. The behavioural component concerns behaviour and experience-influenced attitudes (Antunes et al., 2021). Because people only acquire their attitude from their behaviour or experiences in extraordinary instances, the behavioural component is not included. This only applies when they have a feeble or ambiguous attitude or no other reasonable explanation for their actions. Conflicting cognitive attitudes or a conflict between a cognitive attitude and an emotional attitude can both be components of an ambivalent attitude. Someone who thinks having a VPN is beneficial but also realizes that setting one up is difficult is an example of someone with contradictory cognitive perspectives (Okanlawon et al., 2015). The cognitive and affective aspects of attitude might clash, for example, if a person thinks installing updates is important (cognitive) but feels bad or annoyed when they think about doing it (affective). Since effect and cognition make up a person's attitude, these two elements are examined separately in this study.

Because they frequently use computers carelessly and even recklessly and spend a lot of time using technology, students are thought to be one of the computer user profiles most vulnerable to cyber attacks (Chandarman & van Niekerk, 2017). People are more exposed to online hazards of their continuous psychological urge to stay connected via an expanding array of technological gadgets. Students must influence young people's perspectives and encourage them to act morally and wisely online. New information and experiences are filtered for meaning through attitudes and beliefs. Students can only be safeguarded from internet risks if they are informed and enthusiastic about learning about online safety (Okanlawon et al., 2015). There is a strong inverse relationship between dangerous cyber

security behaviours and cyber security attitudes, with more unfavourable views associated with higher levels of risky behaviours. Although attitude is a crucial consideration when creating behavioural treatments, various attitudes require different approaches from interventions. Therefore, it is important to consider attitudes regarding cyber safety and how they impact the overall degree of cyber safety. Internet addiction and impulsiveness are closely associated with hazardous behaviours, and attitudes toward cyber security were adversely correlated with people's engagement in risky behaviours. Young adults reported high levels of trust in their capacity for self-management. They showed a greater concern for social privacy risks than corporate and governmental access to personal data (Okanlawon et al., 2015). Younger teenagers are more likely to be worried about potential threats to their physical safety in the social context of information disclosure. In contrast, older teens are more concerned with potential risks to their reputations.

3.5 Cybersecurity awareness

Awareness is the first step in reducing the number of identity thefts and threats to personal information, reducing the risk of their information being compromised. One of the key components of information security is awareness, which encourages good security practices and enhances cyberspace security (Vafaei-Zadeh et al., 2019). The amount of awareness and attitude toward cyber security concerns may thus be determined by understanding the hazards a user encounters on the internet. Cyber security awareness is regarded as a way which can be used to inform users of the internet of numerous threats that they face when they are online, threats to computers, phones and data they have (Quayyum et al., 2021). In the case of the rising use of information communication and technology (ICT), internet users must take note of the dangers they face each time they are online. Information cyber security awareness is a dynamic concept as exposure to risks and threats on the internet frequently changes, and as such, there is a need to be up to date on the threats posed (Vafaei-Zadeh et al., 2019). In this regard, the presence or absence of cyber security awareness makes online users understand or misunderstand the risks and implications of the activities that they engage in (Quayyum et al., 2021). Awareness of users' cyber security is affected by sharing security information, collaborations and different interventions that affect the user's attitude (Vafaei-Zadeh et al., 2019). Information security knowledge positively impacts the intention to comply with regulations to prevent security breaches (Vafaei-Zadeh et al., 2019). However, since the Covid-19 epidemic began, less focus has been placed on the issue of cyber security

awareness, particularly in light of the risks associated with cybercrime at both the individual and business levels (Alqahtani, 2022).

3.6 Cyber safety knowledge effect on cyber safety awareness

Cybercriminals have profited from the chaos brought on by the COVID-19 outbreak and the focus on the pandemic (Chigada & Madzinga, 2021). Cyber safety awareness is hinged on the extent to which people are aware of the risks they encounter and the measures they use to mitigate them (Quayyum et al., 2021). With the ongoing Covid-19 pandemic and increased online teaching and learning use, students are increasingly engaged in online activities. As a result, understanding cyber security may serve as a springboard for university students to become more knowledgeable about cyber safety precautions to apply when engaging in online activities. With that in mind, it is critical to understand their skills and knowledge on aspects such as password use, as they are vulnerable to cyber threats. However, there is a misconception that one will be protecting oneself with a unique password, and there is no need to worry about other cyber security threats (Hunt, 2016). Although it’s a significant good step to create unique passwords, it is not enough to keep the user's information private due to hackers having knowledge and technologies which can decrypt passwords or do a password bypass (Hunt, 2016).

Another critical aspect of cyber knowledge is risk management, which implies that the student or online or technology has to develop a perception of risk such that there can be a development of need to mitigate the perceived risk again. Thus, the perception of risk leads to the development of protective behaviour of the technology user. Cyber security awareness is a good mitigation measure against online attacks that a user can face (Garba et al., 2020). With specific reference to students, studies in Saudi Arabia, New Zealand and Bangladesh indicated that students of various age groups could not identify cyber security terms such as phishing (Alqahtani, 2022; Garba et al., 2020). The lack of knowledge on cyber security can be attributed to the lack of training and cyber security awareness initiatives by institutions of higher learning such as universities (Alqahtani, 2022).

This may be accomplished by including cyber security awareness lessons in university students' courses, especially for first-year students. However, other researchers in the United States have found that students were conscious of their actions, although they are unaware of their data being used elsewhere within and between university systems (Alqahtani, 2022).

From a Nigerian perspective, students have a basic knowledge of cyber security. Still, they are unaware of what to do with their knowledge to secure themselves (Alharbi & Tassaddiq, 2021). On the other hand, it's important to practice good online behaviour by confirming sources and following official announcements (Chigada & Madzinga, 2021).

Some of the protective behaviours which can be adopted by the user conscious of the risk of online engagement are the use of security tools such as virtual private network (VPN), desisting from the use of weak passwords and being on the lookout for likely attacks by not clicking suspicious links (Chigada & Madzinga, 2021). Therefore, with the perception of risks, one can take protective behavior against cyber threats which can be faced (Figure 2.3).

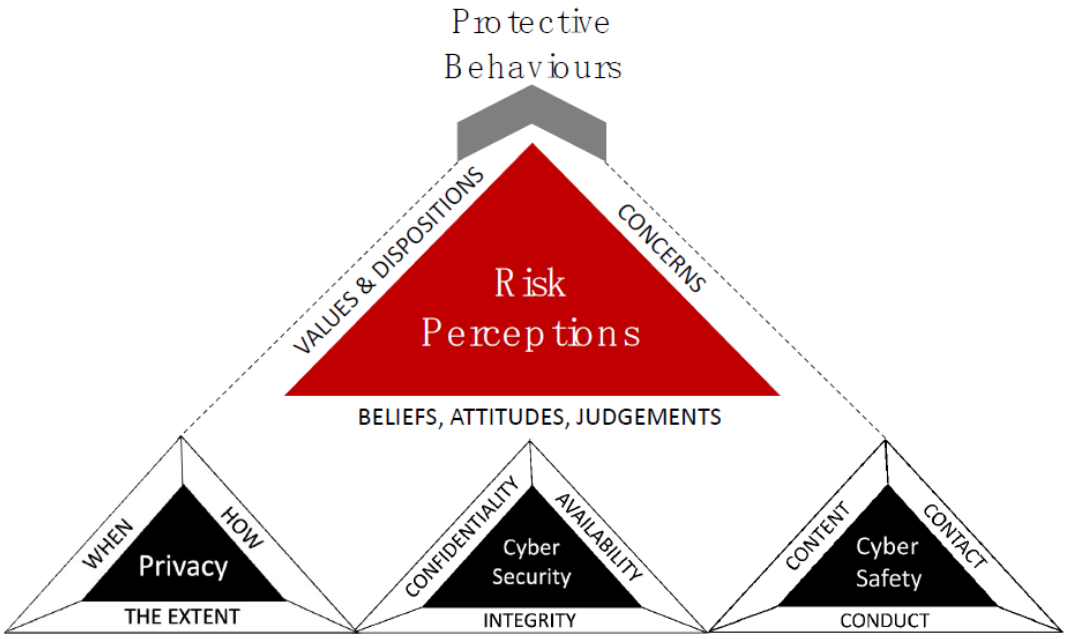


Figure 3.2 : Risk management and online protective behaviour (Source: Tick et al., 2021)

According to Tick et al. (2021), previous studies in South Africa indicated that mobile phone users are vulnerable to attacks as they are less concerned about their cyber security. Due to expense or lack of opportunity, South African students may not have had the opportunity to learn how to utilize Virtual Private Networks (VPNs) (Tick et al., 2021). Collaborations with other countries could increase cyber security awareness among users of online technology, especially by using cross-border training and educational programs. Overall, it should be noted that the availability of knowledge translates to the end user not becoming a victim of cyber threats. For example, Rajan (2010) found out that people still fell victim to phishing

attacks despite being knowledgeable about them. However, the reason for that could be incorrect behaviour towards online security (Chandarman & van Niekerk, 2017).

3.7 Cyber security attitude effect on cyber safety awareness

The outbreak of the Covid-19 pandemic has changed the worldview towards the issues to do with cyber security especially working from home was regarded as the last resort (Wang & Alexander, 2021). It is through the increased use of the internet and online technologies that there is an increased concern about cyber safety awareness. For students, there was increased learning from home during the Covid-19 pandemic, which meant more internet usage and increased time spent online, which meant increased online threats. Some common threats were spam mail, malware, suspicious websites and domains, attacks from Distributed denial of service (DDoS) and social media messaging (Wang & Alexander, 2021).

Internet usage among young people has an impact on their behaviour. ICTs have evolved into a platform for expressing several dangerous online behaviours. Accordingly, dangerous online behaviours include participating in various circumstances that raise the possibility of poor outcomes for oneself or others, such as emotional discomfort, victimization, or decline in social or academic standing (Gámez-Guadix et al., 2016). It's critical to comprehend the influences that might lead certain individuals to partake in these harmful online behaviours. People could not aware of the risks, or they can downplay the dangers of using the internet. Thus, it is expected that people's experiences and knowledge directly affect an individual's attitude. More so, personal attitudes towards user behaviour could be influenced by information security awareness (Vafaei-Zadeh et al., 2019). In this case, user awareness of threats in an information technology context is one of the main predictors of attitude. Information security awareness can increase the user's security precautions. Consequently, individuals will have a more positive attitude. Based on the Theory of Planned Behaviour, it is expected that information security awareness influences the attitude towards having more intention regarding using anti-malware software.

The theory of planned behaviour (Ajzen & Fishbein, 1980; Ajzen, 1991) contends that subjectively perceived standards are crucial in explaining specific types of behaviour. These factors, along with the person's attitude toward the behaviour and the perception of behavioural control, affect the intention to engage in the suggested behaviour (Festl et al., 2013). Generally, an individual's desire to engage in behaviour should be higher the more

favourable the attitude. The subjective norm is toward the behaviour, and the larger the perceived behavioural control. Therefore, the idea that children understand the digital world better as they get older and experience it can impact how they behave online. However, it is far from certain that having a critical understanding of the digital world leads to cautious behaviour when protecting personal information. The results do indeed highlight the disparities in children's digital literacy. For instance, while browsing unfamiliar websites, more than 35% of 12- to 15-year-olds are wary of their privacy and data sharing (Livingstone et al., 2017). Young people believe that if they no longer want to share information with others, it can be erased from the internet. As a result, young people who hold such ideas act whatever they choose online, thinking that nobody else can see what they are doing.

Online behaviour is one such scenario that calls for collaboration across several spheres of assessment, whether harmful or healthy. Information from the social and moral domains will be utilized to direct young people in decision-making processes depending on the collected interpretation of prior encounters within social situations. Thus, when presented with a circumstance requiring moral judgment, whether online or on a mobile device, a teen considers data from social and moral domains before selecting which course of action to pursue. This becomes clear when examining how young pupils may respond differently in analogous situations or how moral ideas vary across various civilizations.

3.8 Summary

The research problem was due to increased online usage due to Covid-19; there has been a change in how education systems have been operated. The Covid-19 pandemic shifted teaching and learning from physical to online and blended learning. Risk management was discussed as one of the most important variables leading to behaviour change among online users, especially during the Covid-19 pandemic, which has seen working from home as the new norm, met with increased cyber-attacks.

The chapter examined the literature on cyber safety knowledge, attitude, and awareness. The chapter looked at the theory that looked at how cyber knowledge and cyber safety attitudes affect cyber safety awareness. However, there are different forms of cyber safety attitudes, and how they affect awareness differs. These need to be separated when changing an individual's attitude towards cyber safety awareness. The attitude of students when engaged

in online learning, the attitude of students can lead to their vulnerability and how the attitude towards threats leads to protective behaviour.

The next chapter looks at the requirements for developing a cyber safety framework among university students. This chapter is central to the study as it looks at how the online risks faced by students can be minimised, thereby making them acquire cyber safety. The NIST framework is reviewed, determining the tiers relevant for developing a cyber safety framework for organisations such as universities.

CHAPTER 4

ESTABLISHING THE REQUIREMENTS FOR CYBER SAFETY AWARENESS

4.1 Introduction

The previous chapter looked at the definitions of the terms such as cyber safety, cyber attitude, and cyber awareness. From the chapter, it was noted that there are several cyber safety attitudes that a student has, and these need to be dealt with separately to improve the cyber safety awareness of students. Training and campaigns have been noted as the main strategies to improve the cyber knowledge of university students, with anticipated protective behaviour and improved cyber safety awareness. However, some challenges lead to negative relationships between knowledge, attitude, and cyber safety awareness.

With the challenges identified from the previous chapter in mind, this chapter looked at the measures that students can use to reduce online risks while, at the same time, increasing cyber safety awareness. The chapter asked the following question: What measures can be developed to address cyber safety awareness challenges among first-year students in Eastern Cape? The chapter intended to develop measures for addressing cyber safety awareness challenges among first year students in Eastern Cape. In order to answer the research question and the secondary objective, the chapter, there was an explanation of the NIST cyber security framework, which guides organisations to protect information and reduce risk. The chapter discusses the tiers of NIST that an organisation can adopt for cyber safety focusing on the major limitations, such as the costs of acquiring the infrastructure. It should be noted that the chapter discusses the aspects of NIST that are relevant to the student's protection from different forms of online risk.

The chapter also discusses the theory of planned behaviour and social learning theory in explaining how cyber safety knowledge can affect cyber attitudes and online behaviour. The chapter also discusses the influence of games and mobile applications to increase cyber safety awareness by doing.

4.2 Global efforts in cyber safety awareness

There are over 2 billion internet users worldwide, thus making the internet part of everyday life and making young people internet users 24 hours a day, seven days a week (Alotaibi & Mukred, 2022b). The more time spend online, the more they become vulnerable to cybercrime and violence. More so, with the internet linking billions of people, issues of cyber security awareness are becoming increasingly important (Vafaei-Zadeh et al., 2019). This is important to develop infrastructure that offers protection to society. Concerns among cyber security specialists who believe the incidence of cyber-crimes is fast rising during the health pandemic have increased due to the global economy being affected by the COVID-19 pandemic and cyber security warfare (Chigada & Madzinga, 2021).

About 80% of Americans between the ages of 18 and 24 use several social media platforms, with 94% of them using YouTube, 80% using Facebook, 78% using Snapchat, 71% using Instagram, and 45% using Twitter (Bhatnagar & Pry, 2020b). There is a high level of use of online social media platforms, making users more vulnerable to attacks in different forms. There is a need to invest in cyber safety awareness among information technology users to reduce cyber-attacks. The levels of awareness can be increased through the idea of digital literacy. There is a provision for different forms of coping with threats from information technologies (Ata & Adnan, 2016). In most Economically Developed Countries (MEDCs), cyber safety awareness is already integrated into their schools' curriculum. For example, the United Kingdom (UK) government has provided education for 11–14-year-olds on how they can be protected online (Kritzinger, 2017). Young people must thus be educated on cyber safety concepts that safeguard them and their surroundings from potentially harmful situations. Therefore, this study must ascertain how much high school pupils know about cyber safety measures.

Cyber safety awareness is taught in other MEDCs, such as the United States of America, New Zealand, and Canada (Kortjan & von Solms, 2014). However, the case is different in the least Economically Developed Countries (LEDCs), with references mainly to Sub-Saharan Africa, which is viewed as lagging in cyber safety knowledge (Kritzinger et al., 2017). Grobler and Dlamini (2012) indicated that access to the internet is increasing in Africa. There is limited knowledge and skills in cyber safety awareness, making the user vulnerable to several online risks. However, in MEDCs, some measures are being initiated toward cyber

safety among students, for example, in Tunisia, Rwanda, and Mauritius (Asanan et al., 2017). However, most African countries, such as Uganda, Sudan, Egypt, Morocco, and Kenya, have not developed proper cyber safety awareness within the education systems (Yilmaz et al., 2017b). With specific reference to South Africa, there is an increase in cybercrime rates (Yilmaz et al., 2017b). Thus, it needs to be seen which measures can be taken to reduce the challenges associated with the students' online risk behaviour and the effectiveness of the criteria used to promote cyber safety awareness amongst first-year students in South Africa. It also needs to be determined what strategies will be used to reduce the challenges affecting first-year students' cyber safety awareness. The use of education can be combined with implementing the South African National Cyber Security Policy Framework (NCPF), whose thrust is cyber security education. According to the NCPF, there is a need to create an enabling environment for cybersecurity education and guide the implementation and development of an environment that fosters cybersecurity education (Waldock et al., 2022). However, the South African curriculum currently needs a cyber safety or security curriculum that includes computing and is available for ages 16 and 18 (Waldock et al., 2022).

4.3 NIST cyber security framework and ISO/IEC 27001 standard

The National Institute of Standards and Technology (NIST) developed the cyber security framework. This framework is a high-level program that institutions can use by providing best practices, guidelines, and standards to protect information systems and the data stored therein (Custodio & Malawit, 2020). The researcher used it as a third theory to guide the development of the cyber safety framework for first year university students. The thrust of NIST is to provide training, education, and security policies regarding cyber security awareness (Chandarman & van Niekerk, 2017). It provides organisations with a plan of defence. The thrust of the NIST framework is to reduce the levels of cyber security risks online users face. The other purpose of the framework is to mitigate and reduce risks associated with cyber activities by several actors and adversaries. The framework postulated that there are differences between organizations; they face unique risks from different threats, and all of these need diverse strategies to deal with them. Like any other framework, NIST has a set of controls or activities that must be engaged in for the organisation to comply with it. The main elements of the NIST framework are the framework core, implementation tiers, and framework profiles. However, the NIST framework is not a one-size-fits-all approach to managing cyber security risk for critical infrastructure. Organizations will continue to have

unique risks—different threats, vulnerabilities, and tolerance. They also will vary in how they customize practices described in the framework. Organizations can determine activities important to critical service delivery and prioritize investments to maximize the impact of each dollar spent. Ultimately, the framework aims to reduce and better manage cyber security risks.

Under the framework cores, several activities need to be done to meet cyber security outcomes. The functions, in this case, are to identify, protect, detect, respond, and recover. In other words, the NIST frameworks for risk management and security put us in a position to make informed decisions. More so, NIST provides the probable controls that can be used to achieve the intended objectives and do not dictate to organisations how they should adopt the mechanisms. Therefore, the implementation tiers consist of four sub-elements: tier 1 (partial), tier 2 (risk-informed), tier 3 (repeatable), and tier 4 (adaptive) (Figure 4.1).

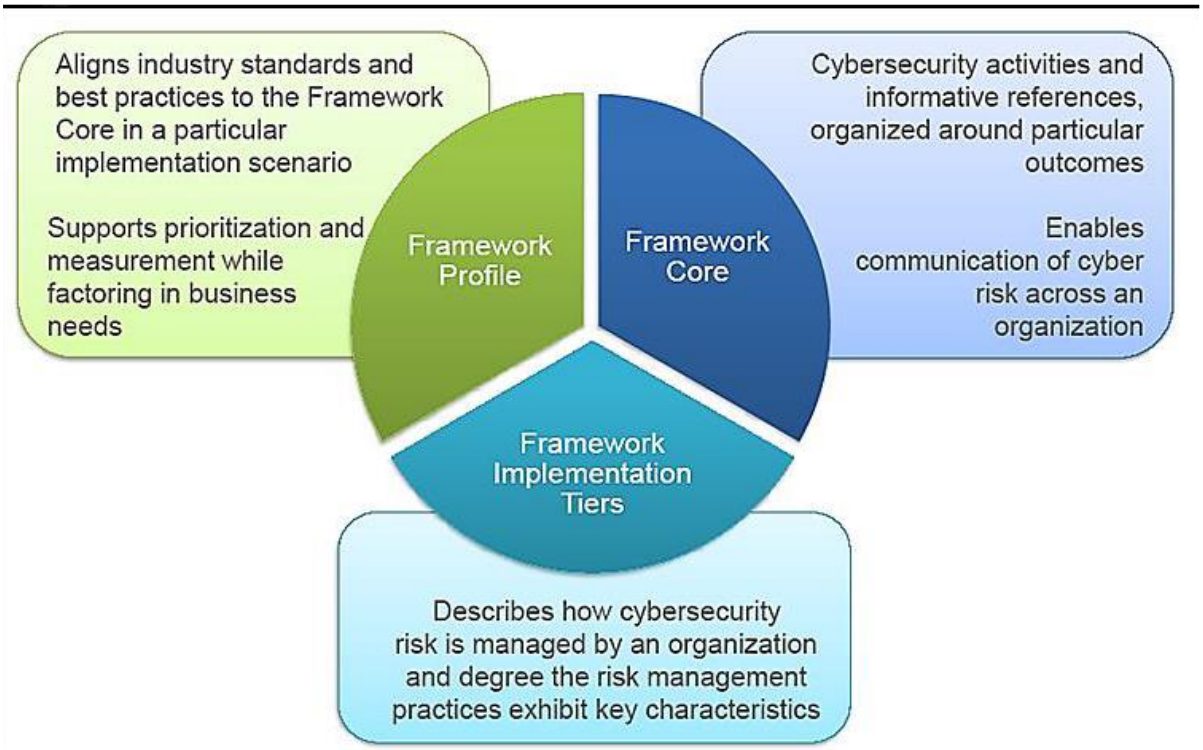


Figure 4.1: Elements of the NIST framework (Source: Custodio & Malawit, 2020)

Organizations at Tier 1 (partial) need a formalized integrated cyber security risk management process and tend to be reactive rather than proactive toward cyber risk management. In addition, organizations at Tier 1 tend to have little interaction with other firms and professional cyber security groups (e.g., an Information Sharing Analysis Center) concerning

cyber security risk management. Tier 2 (risk-informed) organisations tend to have a formal, loosely integrated risk management process, but enforcement of the process as an organization-wide policy is lacking. Tier 2 organizations also tend to have limited interactions with other firms and professional cybersecurity groups concerning cybersecurity risk management (Custodio & Malawit, 2020).

Tier 3 (repeatable) organizations have formal, integrative risk management processes as well as formal channels of communication with other firms and professional cyber security groups concerning cyber security risk management. These organizations are proactive and reactive in terms of cyber security risk management (Custodio & Malawit, 2020). Tier 4 (adaptive) organizations have formal, integrative risk management processes and formal communication channels with other firms and professional groups concerning cyber security risk management. In addition to the proactive and reactive approaches, Tier 4 organizations take an adaptive approach to cyber security risk management. Thus, these organizations continuously monitor changes in the cyber security threats confronting them and revise their recovery plans to accommodate these changes. The financial and operating implications of the requisite changes in the recovery plans are also explicitly considered by organizations at Tier 4 (Custodio & Malawit, 2020). The four tiers associated with the NIST Cyber Security Framework provide organizations with an overview of how to view their cyber security risk management process and what needs to be done to move to a higher tier. The tiers also provide a vehicle for analyzing the financial commitments associated with an organization’s cyber security risk management approach.

Although higher tiers indicate a higher level of rigour and sophistication in cyber security risk management, it does not necessarily follow that all organizations should strive to be at the highest tier level. The benefits derived from reaching a higher tier are not free. In other words, higher costs are associated with moving to a higher tier level. Thus, the appropriate tier is organization-specific and dependent on an organisation's cost-benefit aspects of the cyber security risk management process (Custodio & Malawit, 2020). The tiers describe the organisation’s cyber security methods and implementation within the framework. It is not compulsory for organisations to move through all the tiers but to select the tier that makes them meet their cyber safety and security objectives. Organisations then need to make a cost-benefit analysis to determine the resources at their disposal to provide the requisite security for their end users.

The framework element is the profile, which is the selection of the functions they want to fulfil. There is the current profile, which refers to the current state of cyber safety and security, and the target profile, which is the stage at which the company intends to end up. Individuals and organisations will face unique risks or threats and have different mechanisms to tolerate the threats, and at the same time, there are differences in the level of vulnerability. Therefore, how individuals and organisations deal with threats varies depending on their knowledge of threats and the extent of vulnerability (Custodio & Malawi, 2020). There is no one-size-fits-all solution for the measures that can deal with student cyber-crimes in their day-to-day learning. Generally, the idea is to keep the students aware of the risks they face in online learning.

In this study, the NIST framework was used in order guide the development of a cyber safety framework for first year university students. Basing on the views of Custodio and Malawit, (2020), the NIST framework is a high-level program that institutions can use by providing best practices, guidelines, and standards to protect information systems and the data stored therein. Thus, specifically for this study some of the elements of the NIST framework were adopted for universities used in the study to provide guidance on how the students and institutions can protect information systems. The NIST framework suggests several factors that can be used to develop a cyber security framework. The human-centred ones include human factors, the role played by awareness and campaigns, governance, policy, and technical skills. Human factors define how one perceives risk, which leads to the types of online behaviour in which one engages on the internet (NIST, 2018). In this case, the humans referred to here were the first year university students and university information systems data managers. Therefore, the NIST framework is a source of critical success factors for developing the cyber safety framework. Therefore, the NIST framework was used for the discussion of the research findings, identifying the critical success factors and the cyber safety framework.

4.4 Measures which can be developed to address cyber safety awareness challenges among first year students

Enterprises worldwide are experimenting with working online and from home, which has made the subject of cyber security and the management of cyber risk by individuals much more urgent overnight (Tick et al., 2021). To protect students online in a dynamic

technological environment with constantly changing hazards, sustained efforts are needed from all interested parties. There have been active participants in the policy and practice of online student safety, including concerned policymakers, parents, educators, professionals, and law enforcement authorities. There are demands for limitations on teen Internet use, and enforcing rules and regulations for teen computer use would limit its use, as the use of the internet by kids has raised concerns among educators and the media (Al-Badi et al., 2016). Monitoring computer and internet usage can help decrease pupils' exposure to inappropriate internet behaviour and lessen the impact of negative online behaviour among them.

The greatest way to safeguard today's youngsters is to take steps to filter and ban unlawful and immoral websites. Parents have a crucial role in reducing the risk the internet can provide to their children by monitoring and correcting some information, particularly that of social media networking sites, with their unstructured and unsupervised peer content. Setting up rules for internet use at home, being responsible with how much time is spent online, choosing the right place for the computer, and keeping an eye on the information downloaded might help reduce these hazards.

Before they become students, it is crucial to educate them about the risks associated with the internet since one of the most noticeable shifts in young students is the transition from parental obedience and commitment to peer orientation (Schilder et al., 2016). The training also debunks the misconception that the installation of anti-virus is enough to protect their electronic gadgets and that firewalls are synonymous with anti-virus (Mishna et al., 2010). It seems crucial to intervene at, or just before, the transition toward early students, even though taking risks is a developmental necessity and generally inevitable in early students. During this same stage, they frequently begin independently browsing the internet. Along with keeping an eye on their behaviour, parents must educate their children about the risks of sharing personal information with strangers online and the sites they should avoid. In the browser program, they may keep an eye on their search history. Children should get guidance from their parents on responsibility and internet safety. Although many kids have access to the Internet 24/7, this link also has to be monitored and managed. Law enforcement should utilize their authority to bring legal action against those who hurt kids online. Teachers or other adults at the school should advise pupils about proper Internet usage in a classroom setting.

Parenting strategies must balance shielding children from online harm and preserving the educational, social, and creative opportunities that digital media offers them. This is because opportunities and risks are associated with students using digital media (Livingstone et al., 2017). To mediate their children's access to and usage of digital media, parents employ a variety of tactics, including both restrictive and enabling mediation strategies. These conflict resolution techniques can be divided into four groups: using technical tools like content filters, PIN/password protection, safe search, and other forms of technical mediation; regularly discussing risk management with the child; setting rules or limitations for online access and use; and monitoring children while they are online (Livingstone et al., 2017).

Research and conventional behaviour modification theories support the notion that raising awareness can modify behaviour. According to Ajzen's (1991) Theory of Planned Behaviour, a person's intention to engage in a behaviour influence that behaviour. The attitude of a person with specific views and values regarding the results of the behaviour, subjective norms based on normative beliefs, and his perceived behavioural control that depends on control beliefs all impact behaviour intention. According to this behavioural theory, it may be crucial to provide knowledge to alter attitudes toward the desired behaviour. Prochaska et al. (1998) also argue for the significance of information supply in the trans-theoretical stages of the change model. This paradigm recommends that individuals improve their behaviour in numerous stages. A planned intervention is necessary to move past the initial phases of the paradigm towards behavioural change. One strategy is to raise risk awareness, for instance, through educational materials and behaviour-related information (Prochaska et al. 1998). Both models emphasize the significance of education and awareness campaigns to encourage behavioural change, in this case, to lessen risky internet behaviour. Thus, it appears that there is a rising need for an obligation on the part of institutions to provide instructional and preventative initiatives about harmful Internet use. When you consider that learning is the primary online activity that students report engaging in, this becomes even clearer (Livingstone and Haddon, 2009). According to this research, schools should try to educate all students about appropriate internet usage, as they have the means to do so.

Digital literacy is the capacity for people to use their skills, knowledge, and understanding to take full advantage of the opportunities presented by the new media environment and to protect themselves from related hazards (Livingstone et al., 2017). Digital literacy and media education programs have had a mixed history in the UK (Livingstone et al., 2017), and there

have been new demands to integrate digital media education into the curriculum firmly. Consequently, even when students get a better grasp of the digital world as they become older and more experienced, it is far from certain that this critical awareness will lead to careful behaviour regarding the security of personal data.

4.4.1 Games and mobile applications for education and awareness

Children and young people now have more access to the internet, where they are at risk of various dangers. Numerous safeguards have been implemented; as a result to ensure that users of all ages are protected against various risks. Digital game-based learning is one of the most efficient ways to enthral and motivate users (DGBL). Digital serious games may prove useful for educating this population about security concerns more effectively [6] and in a more individualized way to foster a security culture. Giannakas et al. (2016) created the Cyber Aware mobile app to raise students' knowledge and awareness. Cyber Aware was created for K–6 educators and may be used to enhance formal and informal learning activities indoors or outdoors. This was developed against an increased focus on technological aspects such as game implementation, neglecting the educational side of cyber safety. The mobile application aimed to increase students' understanding of cyber security aspects for internet safety and protection against threats. The topics covered in the mobile application included firewall technologies, antivirus software, security updates, email spam filtering, legacy threats, malware, spam, and cyber-attacks (Giannakas et al., 2016).

The student selects a learning topic and then goes through several games, motivating the individual to complete the game to get security rewards associated with going to the next level. Completion of the game implies that the winner gets a certificate. The Cyber Aware game aims to help the user gain new knowledge by following a problem-based approach and increasing their critical thinking level (Giannakas et al., 2016). The elements of the Cyber Aware game included the first mini-game (Figure 4.2A), which was supposed to be played to gain information about cyber security technologies. In the second mini-game, the player uses the right technology and value to keep the device safe (Figure 4.2B). After passing through the different stages of the mini-games, the mini-games are unlocked in the "arena security" (Figure 4.2C). Arena Security makes the user use the knowledge gained to identify the threat and select the correct data security technology to deal with the threat.

Figure 4.2: Elements of the Cyber Aware game (Adapted from Giannakas et al., 2016)

The third mini-game makes the student figure out the security technologies needed when dealing with specific online challenges based on real-life situations (Giannakas et al., 2016). Thus, the whole essence of the game is for the student to associate knowledge gained through interacting with the mobile application with real-life scenarios. Evaluation of the Cyber Aware application by the authors showed that 61% of the students stated that the message application is fully informative, 67% indicated that they did not face problems when playing the game, and 44% stated that they did not read other material about gameplay. More students (82%) would play the game again at school, and 85% would play the game at home. From the study, it was shown that game-based learning increases the knowledge and awareness of the students towards cyber security. Other online games include “PhishGuru”, which presents story-based anti-phishing educational material to alert people of phishing attacks through email. An online game has also been developed called "Anti-Phishing Phil”, which teaches end users how cues from URLs can help them avoid becoming victims of phishing. The most commonly used awareness training is training, which can be in the form of informative videos, interactive presentations with storytelling, digital comics, making a school curriculum, developing and using tools, and best practices for password generation, use, and changing (Quayyum et al., 2021). The training on phishing can be provided by

providing signs of a phishing attempt, such as misspelt words, a certain degree of urgency or deadlines, fake names and web links, and a request for personal information (Hunt, 2016). The different methods aim to increase cyber safety awareness of different online risks.

4.4.2 Training as a measure of increasing cyber safety awareness

The literature review noted that most universities across the world, South Africa included, did not offer training to students and their educators when they switched from physical to online classes. This meant that the educators and the students were exposed to different levels of cyber threats, especially due to the increased online presence of university students. Increasing cyber security awareness through training programs that expose students to cyber security defence tools through theoretical lectures and simulations (Custodio & Malawit, 2020). These would emphasise the operational, use, and procedural elements of enhancing user comprehension and turning it into efficient cyber security mitigation behaviour. For instance, a well-liked training tool called "Phishing Simulator" was created as an effective training procedure to raise awareness of suspicious emails sent by hackers (Zwilling et al., 2022). Such emails frequently contain harmful software, or "malware," which causes unauthorized data leaks. The simulator is also appropriate for instructors, providing them with access to useful security tools to reduce phishing emails and internet links and directing them to achieve the highest levels of defence against cyber security risks (Antunes et al., 2021). Initiatives help people become more aware of and knowledgeable about cyber hazards.

Training is there to improve the cyber safety knowledge of internet users, for example, through training initiatives aiming to increase users' understanding of and sensitivity to possible cyber security risks (Quayyum et al., 2021). Before and following cyber security training, trainees concentrate on knowledge of password protection and the capacity to safeguard computers. Campaigns to raise awareness may help curb online risk-taking. Training provides the students with knowledge on how to use complicated passwords because of their exposure to and experience with them in training programs (Alqahtani, 2022). Offering security awareness training programs might significantly impact people's attitudes toward information security management (Quayyum et al., 2021). The training style should be determined by a combination of delivery techniques (such as text-based, game-based, and video-based). Courses on cyber security should be problem-centred and include case studies appropriate for the student's knowledge levels (Wang & Alexander, 2021).

4.5 Related work on cyber safety awareness frameworks

Due to the Covid-19 pandemic, online frequency and online risks of online users increased and there has been an urgent need to protect users through the development of safety guidelines and frameworks (Siyam & Hussain, 2021). In the study in Dubai by Siyam and Hussain, (2021), the motivation to carry out the study was the absence of a cyber safety policy or framework for students at private schools. The study managed to identify the factors to be adopted for application into schools which is different from this study which focused on university students.

Tsokota et al., (2022) determined a strategy to enhance e-safety among 1st year students in Zimbabwean university students. The similarity with the current study was that the study focused on university 1st year students. The study was motivated through the exposure to risk and the students not prepared to e-safety. The study used action research to identify the strategy whilst this study used mixed method research to develop a framework for cyber safety awareness among first year university students. The main finding was that knowledge about e-strategies was low and that education was critical in e-safety. The centrality of education in the development of e-strategy makes it be considered as a critical success factor for the development of a cyber safety framework.

Kritzinger et al., (2019) cheap prizes of ICT devices and noted that school learners used cyberspace for socialization and education. The differences with the current study is their target on the school learners whilst the present study is on first year university students. Lack of cyber safety awareness, skills and knowledge about information protection in the cyber space is limited. There are similarities in the use of mixed methods approach. Like Tsokota et al., (2022), these authors made of use of game based learning to make students aware of the challenges which they face in the cyberspace. The conclusion reached by Kritzinger et al., (2019) was the inclusion of cyber safety awareness, education, knowledge and skills need to be part of the school curriculum to allow school learners to protect themselves.

Scholtz et al., (2019) looked at the requisite resources, knowledge and skills of the educators in South African school as a measure of enhancing cyber safety awareness due to absence of cyber safety in South African school curriculum. The study was based on a scoping review and expert review panel were used to review the validity of the proposed framework. The differences with this study are that it was focussed on educators and not the students and also

in schools and not at university level. The authors proposed a theoretical framework based on the Jahoor Dimensions Digital Literacy Model composed on technical, social-emotional and cognitive dimensions. The elements relevant from their framework was ICT literacy, online etiquette literacy and cyber safety literacy. The conclusion for the study was proposal of a theoretical framework to create and enhance cyber safety awareness in school.

Paraiso (2019) looked a cyber safety information framework for parents in South Africa. The thrust of the study was to provide parents with cyber safety information which is not similar in this study were the thrust was providing safety awareness to the student.

4.6 Critical success factors for cyber safety awareness among university students

The crucial success factors (CSFs) were proposed based on input from the experts on the preliminary framework for cyber safety awareness in Section 7.3. To implement the reviewers' suggestions, an extensive review of the literature in the area of cyber safety is needed. To make the framework student-centred, their perceptions, which were collected using questionnaires, were factored into the development of the CSFs. To this end, the researcher looked at the different publications that identified some of the CSFs needed to develop a cyber safety framework. The variables such as cyber security knowledge and attitude, online risks faced by the university students and the measures intended to reduce the challenges which the students face were the context. An explanation of the context were the factors which need to be taken into account to improve the cyber safety awareness of the university students. The identified factors above were used in the development of the initial model for cyber safety awareness which were given to the experts for further review. Table 4.1, some new issues added were educational campaigns, human factors, mitigation measures, social factors, and governance issues, especially with policies and regulations.

Table 4.1: Critical success factors for cyber safety awareness among university students

Critical Success Factors		Literature Review		Theory	References chapters
Context	**Factor (s)**	**Description**	**Reference (s)**		
Knowledge capacitation	• Knowledge • Attitude • Risk perception	• Train the students to know the cyber threats • Include cyber safety into the university curriculum • Play game models to learn through play	(Almaiah et al., 2020; Bada & Sasse, 2014; Gundu et al., 2019; Lallie et al., 2021; Richardson et al., 2020; Vafaei-Zadeh et al., 2019)	• Theory of planned behaviour • NIST	• Chapter 1 Section 1.6.1 • Chapter 4 Section 4.3
Attitude	• Password strength and protect • Internet trust • Downloading sites	• Provide policies which prohibit students from accessing certain sites • Carry out awareness campaigns about the benefits of password strength	(Almaiah et al., 2020; Choejey et al., 2016; Gundu et al., 2019; Lallie et al., 2021; Richardson et al., 2020)	• NIST	• Chapter 4 Section 4.3
Risk/time awareness	• Identity theft • Sexting • Bullying	• Provide information on university websites about online behaviour and restrictions • Inform students through workshops about the dangers of spending too much time online.	(Choejey et al., 2016; Gundu et al., 2019; Vafaei-Zadeh et al., 2019)	• NIST	• Chapter 4 Section 4.3

Based on the recommendations by experts, the review showed that the human factor and training and awareness campaigns are some of the most important factors affecting university students' cyber safety awareness. However, although not referenced by most authors, students tend to develop trust in what they find on the internet, making them vulnerable to cyber-attacks. One must translate technological skills into knowledge of the security issues that must be dealt with online. The need for governance, which can be in the form of policies and regulations that govern the students' online access, was one of the factors that students indicated when responding to questionnaires. All the above success factors were there to increase the knowledge and skills of the students when surfing the internet and, at the same time, change their online behaviour and perception of online risks. When examined in combination, these factors affect the cyber safety awareness of the students.

Based on the results presented in Chapter 6, some of the measures that the students indicated were based on the mean scores of the Likert scale. 1.64 is less than half of the students and as such one cannot deduct that the students agreed. The students agreed (mean=1.64; standard deviation=0.59694) that they needed training programs about how to protect themselves from cyber-attacks as they were some who had shown that they had less knowledge of cyber security. Results also indicated a need to develop a cyber security policy or framework that the university or communities can follow to reduce the number of cyber attacks among university students. The need to frequently change the password (mean = 1.9704, standard deviation = 0.73285) was a skill the students needed to have to be safe while they were on the internet. Adding to the factors derived from the review, awareness campaigns and training, technical skills, and availability of a cyber safety policy are the ideal factors for the regulation of usage of the internet by the students.

4.6.1 Review of the critical success factors by experts

Since the experts adopted the recommendations, they needed to see the CSFs developed from the literature review and findings based on the student's perceptions (see table 4.1). In this case, the two experts used in developing the initial framework were used again to review the CSFs. Like in the first framework to be developed, the reviewers asked for the dominant CSFs and the intersection with the findings from the questionnaires administered to the students. The common issues from the questionnaires were mitigation measures in the form of technical skills, the need for training and awareness campaigns. From the review of the

literature, the common theme was centred on human factors (attitude, risk perception, knowledge and skills about cyberspace) and the need for training and awareness campaigns. The researcher noted that skills, training, and human factors were the CSFs central to developing the cyber safety awareness framework for use by university students. However, the reviewers asked for clarity on the trustworthiness of the internet. The researcher clarified that the issue was centred on some students' limited knowledge and that they trusted or did not authenticate some of the sites and information they received on social media, emails, and websites. This implies that they trust most of the things they find on the internet, making them vulnerable to cyber-attacks. Hence, the issue is placed as a technical skill to avoid the reduplication of the CSFs.

4.7 Initial cyber safety awareness framework

The development of the framework was based on extensive literature, as presented in chapters 2, 3, and 4. Out of the literature, the constructs of the framework were identified. The literature identified factors that affect the cyber safety awareness of the students from University X and University Y and the challenges they face in terms of their cyber safety awareness. Chapters 2, 3, and 4 pinpointed the following issues: i) students need to be aware of their own and the action of others and the associated outcomes, ii) knowledge of the precautions they need to take when using the internet, protection of personal data, iii) digital identity and the security measures associated with the use of cyber technologies. Cyber safety awareness also included measures to minimize the risks associated with fraud, privacy breaches, malware, phishing, and scams. Thus, the framework was developed by integrating data collected from questionnaires. More so, the framework presented in Figure 4.3 was as a result of the critical success factors which were identified in literature. Further the critical success factors were presented to the experts' panel for further review. This meant that the refined factors were also added up to the development of the proposed cyber safety framework for first year university students. To relate figure 4.3 to the critical success factors, the variables such as cyber security knowledge and attitude, online risks faced by the university students and the measures intended to reduce the challenges which the students face were the context. An explanation of the context were the factors which need to be taken into account to improve the cybersafety awareness of the university students. The initial framework developed for this research is shown in Figure 4.3.

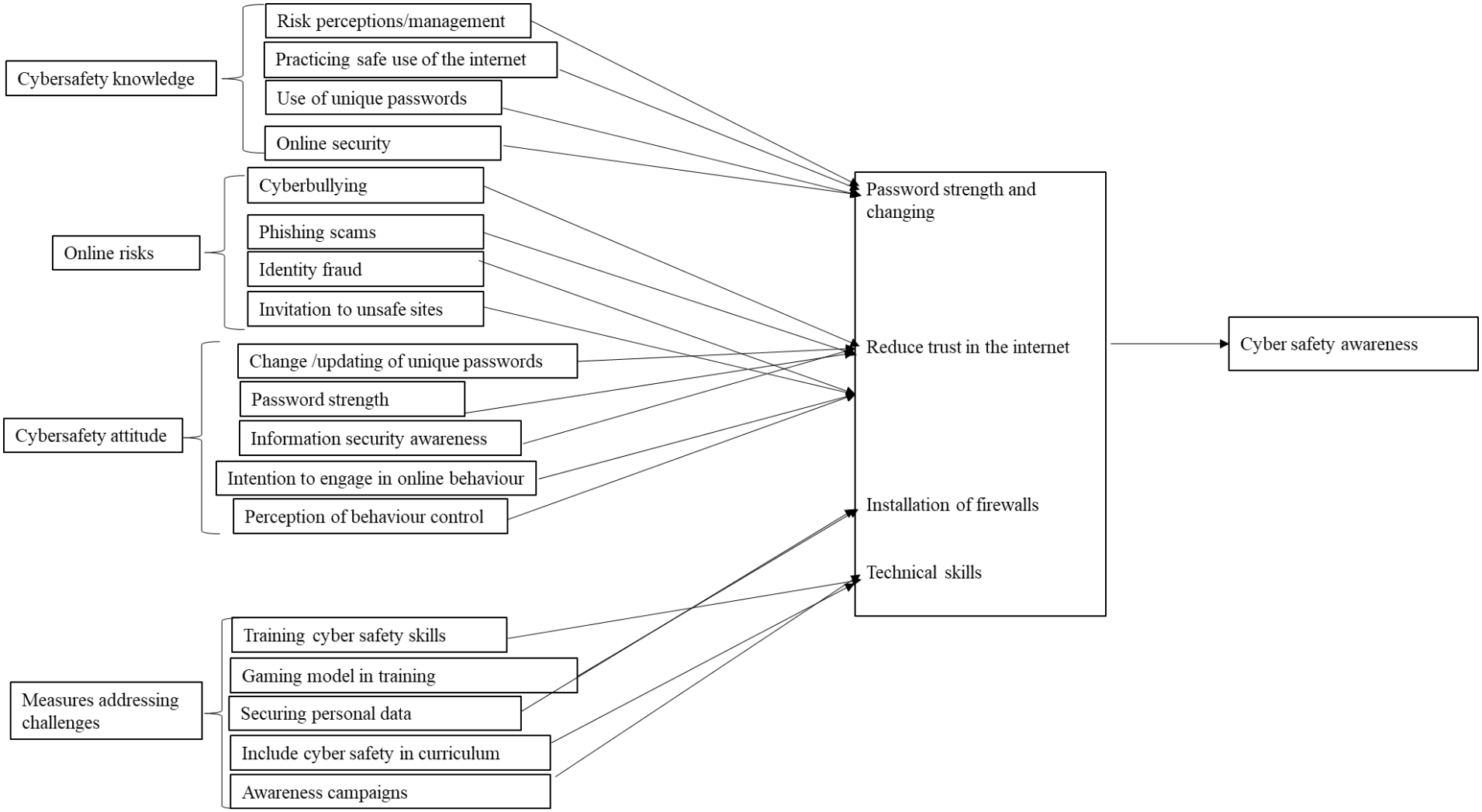


Figure 4.3: Initial cyber safety awareness framework

Figure 4.3 presents different cyber safety challenges students face with online access. The framework categorized the factors into three major elements: the cyber safety challenges faced by the university students, their knowledge of the concept of cyber safety, and individual factors that also affect their level of cyber awareness. Combined, all three factors affected the university students' cyber safety awareness level. Some factors include knowledge of cyber safety, including individual factors such as online behaviour, attitude towards cyber safety, and perception of risk. Under the cyber safety factor, it has been found that students need to protect themselves from having their identity stolen, and at the same time, they need to know about the amount of time they spend online.

However, the increased online presence is not a deliberate move by the students; it is because of the COVID-19 pandemic, which changed physical teaching to online learning and blended learning. All these shifts in learning modes meant that the students were spending more time online, which was met with many cyber threats. The results of the study even indicated that the longer the students stay online, the higher the risk they face. Since some students indicated they had less knowledge about particular risks, they need to know how to minimize the risks they face online. At the same time, knowledge of risks and how to reduce them can be imparted to students. This can be done by including cyber safety components in the university curriculum, especially for first-year students. The students also need to know the security tools they need to have to minimize the risk of online threats.

Under cyber safety challenges, the initial framework covers the challenges the students faced, including the lack of knowledge on online risks. Some challenges stem from lacking an educational foundation or training in cyber safety. The results presented in Chapter 4 indicated that some students do not know cyber aspects such as phishing, sexting, and identity theft. This meant they could not be aware of things they had limited or no knowledge of. With the human being as the link to cyber threat attacks, the lack of knowledge made university students without knowledge of the different risks more vulnerable. This study found that the challenges the students faced online were due to their increased online presence and, more precisely, being online every hour. This implies that students' exposure to online risks increases as they spend more time online. The Covid-19 pandemic has exacerbated the frequency of students online as there has been a shift from physical learning to wholly online and blended learning. This meant that the students needed to be frequently

online to meet the demands of their education while simultaneously exposing them to online threats of different forms.

Moreover, some students do not want to go through security measures. The knowledge of cyber safety in Figure 4.3 depicts the students' cyber safety knowledge. Some frequently discussed states of knowledge include the ways to protect personal identity, the minimisation of online risks they face, and several risk mitigation measures (Quayyum et al., 2021).

There are individual based factors that affect how students engage in online usage. These include their perception of risk and attitude towards the measures used to reduce their online risk. This may be supported by planned behaviour (Ajzen, 1991), according to which an individual's attitude is positively correlated with their behavioural purpose (Vafaei-Zadeh et al., 2019). However, the behaviour can be influenced by the society in which the person lives, which determines whether a person changes (Alotaibi & Mukred, 2022b). In cyber attacks, the human being has been viewed as the weakest link (Chandarman & van Niekerk, 2017; Matyokurehwa et al., 2021), which is based on the level of the different forms of attacks and measures used to reduce the impacts of the threats. Thus, there is a need to make sure that there is depreciation in the weakest link of the human being, and in the case of this study, the students were through several ways, such as training and awareness campaigns. However, (Dlamini & Ndzinisa, 2020b) pointed out that in the South African context, the students began studying online without enough preparation, and their access to digital learning materials is constrained, prohibiting them from achieving the learning goals. When learning during the COVID-19 epidemic, pupils were more exposed to online hazards due to a lack of instruction.

According to Ajzen's (1991) theory of planned behaviour, a person's attitude toward and perception of their ability to regulate it drives them to carry out the behaviour under consideration. In this case, some students had a different attitude towards cyber safety, so their likelihood of doing the same risky behaviour was high. In some cases, it can be assumed that the level of knowledge about online risk would lead to cautious behaviour regarding personal data protection, although there is uneven digital literacy. The need to look at the safety of the students emanates from the view that there are changes in attitude, behaviour, and perception brought about by the changes in technology (Laher et al., 2021b).

4.7.1 Review of the initial model by experts

The experts used in the study were lecturers teaching computer science and information systems with qualifications like doctorates and master's degrees. Therefore, these experts were given a chance to review the initial framework which was developed following the review of literature and was presented in Figure 4.3. The main elements of the initial framework were cybersafety knowledge, online risks, cyber safety attitudes and measures of addressing online challenges. The main elements had some sub-elements as well which made changes to the human trust when online and technical skills which in the end would improve their cybersafety awareness. The need for experts was to give their opinion on the variables included in the initial framework and how they are constructed to develop a cyber safety awareness framework. The experts' main recommendation was that the initial structure aligns with the study's objectives and hypotheses. The main elements of the objectives were: cybersafety knowledge, online risks, cybersafety attitude and measures to deal with the cybersafety challenges. Thus, checking on the initial framework, it can be noted that all the objectives were included in the initially developed model. One of the reviewers suggested including the NIST cyber security framework and ISO/IEC 27001 standard (NIST, 2018). However, the NIST framework mainly targets security and privacy for information systems and organisations. This study adopted the elements of the NIST framework that were relevant to this study, including training and awareness, governance, and policies toward cyber security. The feedback on the framework indicated some missing elements, especially on the challenges that affect the students when the experts thus required online and their viewpoints. Their major challenge with the initial framework was that it was not reflective of the issues based on the students. Although the reviewers indicated that the framework needs to align with the ISO framework, most elements were specifically related to organizations rather than individuals. Thus, the researcher looked at the framework and took out elements related to the students or the human element.

4.8 Summary

The chapter reviewed the different measures which were needed for the development of a cyber safety awareness framework. In this, the NIST framework was reviewed and showed that there are different tiers an institution can adopt to improve the protection of end users

and information. It was discussed that organisations don't need to move through all the tiers of the NIST framework, as this depends on the availability of funds to have the requisite infrastructure. Different countries have made several global efforts to increase cyber safety awareness. The success of the measures varies from country to country based on the differences in the social, economic, and political environments. Games have a participatory approach in which the users can learn the different forms of cyber safety through doing, which improves their protective ability towards the different forms of online threats students face online.

The study aimed to develop a cyber safety awareness framework for university students at selected universities in South Africa. This meant that several measures needed to be put in place to have a framework to deal with the cyber threats that the students faced due to increased online exposure. The elements from the NIST framework relevant to this study were identified and used to identify the critical success factors.

The next chapter presents the research methodology which guided the whole research. The chapter included the population, sampling, data analysis, and ethical considerations.

CHAPTER 5

RESEARCH METHODOLOGY

5.1 Introduction

The first chapter covered the introduction and background of the study, creating a setting for the study and justifying why it is crucial to carry out this study in the wake of the COVID-19 pandemic, which increased the use of online methods of teaching and learning. Chapter 2 reviewed the context and theoretical background of the study and looked at the transition between high school and the first year at university. Chapter 3 looked at cyber knowledge and how it affected the cyber safety awareness of university students. The chapter discussed how games influenced the development of cyber safety knowledge and awareness of the user.

This chapter focused on the research methodology that guided this study. The elements of the methodology were important in determining the problem the study addressed and its main contributions, and how the results are intended to reach a broader audience. In the chapter, there was coverage of the research paradigm, which influenced the research design adopted in the study. Specifically, the chapter discussed the sequential mixed research design used to collect data to develop a framework for cyber safety awareness amongst first-year students in the Eastern Cape, South Africa. The chapter also discussed the selection of the descriptive survey based on the ability to collect large volumes of data while making independent assumptions and detaching the research from the participants.

This chapter also addressed population, sampling, and sample size issues. The sample size was determined using an online sample size calculator, which assumed a certain margin of error and confidence level. The online questionnaire was developed on the Survey Monkey platform, to which the University Y is subscribed. The chapter also discussed that the online form was regarded as the best data collection tool for the ongoing COVID-19 pandemic, as there was minimal contact between the researcher and the participants. Data collection instruments, along with their advantages and disadvantages, were explained. The ethical considerations followed in the study were also discussed. The chapter discussed the data analysis methods, such as the Chi-square test and the test for instrument reliability using the Cronbach alpha test.

5.2 Research paradigm

A research paradigm is defined as a set of views that guide the way of thinking or reasoning of a researcher on how to produce knowledge based on a set of problems faced in society (Gabra et al., 2020b). In this case, the research paradigm is regarded as a research viewpoint that guides research. Specifically, a research paradigm was used to identify the research design used in the study, guide the process in which data was collected, and, in the end, how the data was analysed (Alotaibi & Mukred, 2022a). The research was based on the pragmatism research paradigm emphasizes practical, real-world problem-solving and the importance of combining theory and practice. From a pragmatism perspective, knowledge is context-specific and dependent on the situation in which it is used, and that theories should be judged based on their practical consequences (Bhattacherjee, 2012). The pragmatism paradigm is typically focused on solving specific problems or addressing practical issues, with a strong emphasis on empirical observation and experimentation (Bhattacherjee, 2012). Pragmatists often use mixed-methods approaches, combining qualitative and quantitative data, to gather a rich and nuanced understanding of the problem they are studying. This study used mixed methods as there was collection of quantitative data using online questionnaires and telephone interviews. In this case, the researcher used online questionnaires, which meant there was no contact between the researcher and the students who participated in the study. This meant that data was collected independently without the influence of the researcher. This study used pragmatism to guide the study to understand the students' online behaviour in a university setup and also the critical success factors which are needed to develop a cyber safety framework for first year university students. In this study, there was a need to determine the cyber safety awareness of first-year university students and measure their online risk behaviour and the associated challenges faced in cyber safety awareness. Specifically, in this study, the pragmatism paradigm was vital as it enabled the identification of online risks facing university students at selected universities in the Eastern Cape. Furthermore, the paradigm also aided in determining the level of cyber safety awareness among university students in the Eastern Cape.

5.3 Research design

Bhattacherjee (2012) defined a research design as a strategy used by the researcher to have well-polished research. In other words, a research design is a template upon which research is

based, including the procedures and methods that the study follows to complete the research. Being guided by the pragmatism paradigm, the researcher adopted a quantitative research strategy (Alzubaidi, 2021). A sequential mixed method research design involves gathering both quantitative and qualitative data, conducting separate analyses of each type of data, and then comparing the results to determine if they support or contradict each other (Creswell, 2012). An explanatory sequential mixed design is also called a two phase model which consists of collecting quantitative data and later on collect qualitative data which is used to explain the quantitative data (Creswell, 2012). The study adopted the explanatory sequential design which involves collecting quantitative data first, followed by qualitative data to help explain and expand upon the quantitative findings. Specifically, quantitative data is collected first as it provides an over view of the research problem at hand and provides more robust analysis and qualitative data is there to refine and explain the general overview of the research problem (Creswell, 2012). The purpose of using mixed methods is to provide a more comprehensive and nuanced understanding of a research question or problem, by combining the strengths of both qualitative and quantitative research methods. Mixed methods research design involves collecting and analyzing both numerical and narrative data, as well as using a variety of research tools and techniques such as surveys, interviews, observations, and focus groups (Bhattacherjee, 2012). This allows the researcher to gain a more complete picture of the research topic, by capturing both statistical patterns and trends, as well as the experiences, perceptions, and attitudes of participants. In this case the researcher integrated views from expert interviews and online questionnaires in different stages of the research process such as data collection, analysis, and interpretation. The goal is to use each method to complement and enhance the other, providing a more holistic and rigorous understanding of the research problem. The study adopted the explanatory sequential design which involves collecting quantitative data first, followed by qualitative data to help explain and expand upon the quantitative findings. The quantitative involved a large sample of first-year university students from University X and University Y in the Eastern Cape. The students' views were determined using a Likert scale (Glas & Kleemann, 2017). The Likert scale used numbers ranging from 1-4, as follows: "Strongly Agree" =1, "Agree" =2, "Disagree" =3, and "Strongly disagree" =4. The quantitative data was collected using an online questionnaire from the first-year students on the risks they face online and their level of awareness of cyber safety. At the same time, online questionnaires made the collection of data easy. The study was quantitative data allowed testing how the Theory of Planned Behaviour and Social Learning Theory

would be applicable in determining the level of cyber safety awareness of the students used in the study. To a lesser extent, the study was qualitative as the researcher sought expert views on the critical success factors used to determine cyber safety. The views of experts were used to review the proposed cyber safety framework. Through the explanatory sequential design, quantitative and qualitative findings were integrated in the interpretation stage to provide a comprehensive understanding of the online risks, the cyber safety knowledge and attitudes of the university students. In the study the aim was to use data from expert interviews to expand on the findings from online questionnaires in order to develop a cyber safety awareness framework for university students.

5.4 Research methodology

Research methodology studies the methods adopted in painstaking research to fulfil its objectives (Bhattacherjee, 2012). Therefore, the purpose of any methodology is to aid us in understanding the process of scientific inquiry rather than the results of it (Cohen et al., 2007). The methodology for this study was related to the research philosophy used to govern this specific research. The study technique was utilized to implement the pragmatism research paradigm and create a framework for first-year students at a South African university to be aware of cyber safety. The research used an explanatory sequential mixed method research design which meant that quantitative data was collected first and then followed by qualitative data. The quantitative research methodologies are numerical and entail the collection of numerical data, which needs statistical analysis to accept or reject set-out hypotheses. This study was quantitative as it collected the students' views, which were quantified on a 4-point Likert scale. On the other hand, the researcher collected qualitative, data meaning there are views and perceptions of participants that are non-numerical and presented as narratives. Specifically, qualitative data was collected through the use of expert interviews which meant that the views of experts in computer science or information systems were sought with regards to the critical success factors for cyber safety awareness and their views on the proposed cyber safety awareness framework. An overview of the research philosophy that will direct this investigation, the methods used to gather primary and secondary data, the demographics and sample size for the study, and the ethical standards that will be followed are provided in this subsection, as shown in Figure 5.1.

Figure 5.1 shows the coverage of the research paradigm that was followed and the research strategy that the study followed. In this case, the research paradigm was directly influential in selecting the research design that the study followed. The research paradigm for the study was pragmatism, which means that there was a collection of data with the researcher being detached from the participants, and this meant that this was linked to the quantitative research strategy, which collected numerical data. The researcher also used telephone interviews to collect qualitative data from experts in information systems and or computer science. The population was composed of first-year university students at the selected university, and a sample size calculator was used to determine the sample size. The other part of the population was the experts in cyber safety issues who were selected to participate in the expert interviews. Data from the selected sample was collected using online questionnaires and expert interviews. Quantitative data were analysed using different statistical methods, and based on the findings, a cyber security awareness framework for university students was developed. Data collected using expert interviews was analysed using thematic analysis especially on the critical success factors which affect cyber safety awareness of the university students. The experts were used to give feedback on the proposed cyber safety awareness framework for first year university students.

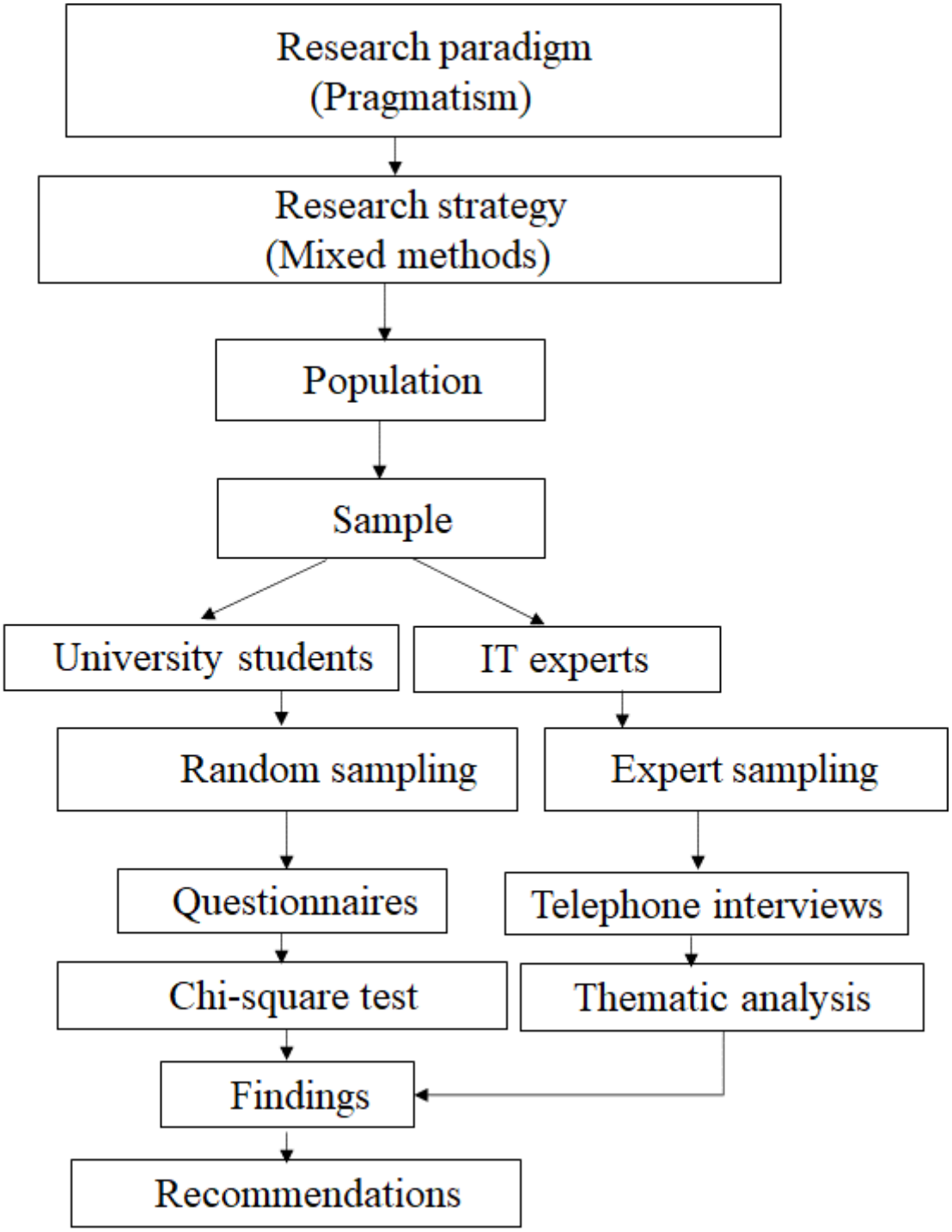


Figure 5.1: Methodology to be used in this study

5.5 Population and Sample

The population is the total number of elements that meet the study's requirements (Cooper & Schindler, 2014). This study dealt with human beings; the population was all the individuals that met the study's requirements. In this case, the individuals who met the required criteria

were first-year students from University X and University Y. Since this study required knowledge of the online risks faced by first-year university students, the populations were all first-year students aged 18 and above from University X and University Y. From the 2022 data, approximately 3021 first-year students were at University Y. No students under 18 were included in this study, as they would have needed consent from their guardians. At University X, the equivalent cohort comprised 1287 students. Thus, the total population for use in this study is 4308 first-year students. This implied that the research used all the first-year students at the two universities, such that there was variability in the measurement of cyber safety awareness for all the first-year university students. Using the first-year cohort implied that the framework would be valid for all students, not just those in a particular department. Like any study, there is a likelihood that it is impossible to make sure that every member of the population is included to participate in the research (Hawashe, 2015). They needed to participate in the study so that their views represented the more significant population from which they were selected. The part of the population used in a study was called a sample. The following subsection presented a description of the sample size.

5.5.1 Sample size

According to Stockemer (2019), a sample is a subset of the larger population used to gather data. As a result, a researcher can draw inferences about the population using information gathered from a larger group. (Shungu et al., 2014). This research proposes using a sample size calculator to determine the sample size for this study. Specifically, the Survey Monkey sample size calculator (https://www.surveymonkey.com/mp/sample-size-calculator/) was used. This was premised on assuming that the population followed a normal distribution with a 95% confidence interval and a 5% margin of error. The sub-population for University Y was 3031 students, and 1287 students came from the University X. Thus, the total population used in this study was 4308 first-year students. Using the sample mentioned above size calculator, the total sample size for the study was rounded up to 450 first-year students to ensure more data was collected and increasing variability in the responses.

Alternatively, the sample size as it allowed to input the confidence interval, proportion and precision and the formula works well with large populations as was the case in this study. Examples of studies who used Cochran's formula include (Bartlett et al., 2001; Bhattacherjee,

2012). The confidence interval =95%, margin of error=5% and proportion was assumed at 0.5. The calculation of the confidence interval was as follows:

$$n= (Z^2*p*(1-p))/E^2$$

Where:
n = required sample size
Z = Z-score for the desired level of confidence (for 95% confidence, Z = 1.96)
p = estimated proportion of the population with the characteristic of interest
E = desired margin of error as a decimal
Assuming that p is 0.5 (a conservative estimate producing a big sample size) then sample size is calculated as:

n = (1.96^2 * 0.5 * (1 - 0.5)) / 0.05^2
n=384

The study used stratified random sampling to select the participants who participated in the study. The two universities were used as strata from which the first-year students were selected. The first stratum was University X, and the second was the University Y. It is from this stratum that the students were randomly selected. Random sampling is an approach whereby participants are given an equal chance to participate in the study (Shannon-Baker, 2016). Thus, in random sampling, participants had an equal chance of being selected to participate in the study. The findings were generalizable to the larger population from which they were chosen.

Since the study was using a mixed method the selection of experts to be used for expert review was guided by Guest et al., (2006). Guest et al., (2006) indicated that sample size for purposive sampling is determined by the saturation concept which means that no new information or data was collected when the sample size was increased. There is no one size fits all on the sample size for qualitative studies but generally a sample size as reaching saturation between 6 and 12 and a maximum number of 30 (Guest et al., 2006). In this study, the experts were selected due to their knowledge of cyber safety. Six people were selected using expert sampling as no new data was being collected by increasing more experts. Thus saturation was achieved when the sixth expert was selected.

5.6 Data collection methods

This subsection dealt with data collection methods, which ensured that adequate data was collected from the students, and the study relied mainly on primary and secondary data sources. Data collection is the process in which the researcher gathers data from different sources, such as the research participants and literature, to answer the research questions or hypotheses (Bhattacherjee, 2012). Specifically, data can be regarded as "primary," collected in raw format from the participants and not analysed to make sense. The primary data was collected from first-year university students and expert reviews in this case. At the same time, secondary data are pieces of information that have already been analysed to produce meaning based on the researcher's demands. This study collected secondary data on cyber safety awareness from journals, books, government records, newspapers, dissertations, and theses.

5.6.1 Secondary data

For the study, secondary data was collected from different sources in the form of peer-reviewed journals, textbooks, and reports that dealt with cyber safety awareness. Thus, secondary data were consulted to get insights about the theories to guide the study and answer the research questions under the literature review. Secondary data was also analysed through the use of content analysis for the most important factors which are related to the development of a cyber safety awareness framework for first year university students. The elements identified through content analysis were then used in the creation of critical success factors the development of a cyber safety awareness framework for first year university students as presented in Chapter 7 for this study.

5.6.2 Primary data

Data for this study was collected through online questionnaires due to the COVID-19 pandemic, and there was less face-to-face contact. Thus, the researcher collected data using Survey Monkey, an online platform. Specifically, the student's primary data collected was the frequency with which they spent online, the online risks that they faced, their level of cyber safety awareness, and the measures that can be used to deal with the challenges relating to their cyber safety awareness. All this was collected using online questionnaires. The following sub-section described and explained the contents of the online questionnaire used to collect data from university students.

5.6.2.1 Online questionnaire

A questionnaire is a tool used to collect data that participants can easily understand, infer, and fill in, which raises the answers the researcher gets from the study (Stockemer, 2019). Stockemer (2019) defines a questionnaire as an instrument comprised of questions filled out by respondents themselves. The study used an online questionnaire on cyber safety awareness that met the demands of the current research. Specifically, the questionnaire collected data from randomly selected first-year students in the Eastern Cape. The researcher used a Survey Monkey questionnaire consisting of interactive forms to collect data. The students received an email requesting that they take part in the study. This type of survey was cheap to carry out since the results are instantly recorded in an online database, and modifications are made to the questionnaire if required.

Questionnaires are usually regarded as research tools that generate findings that can be generalized to larger samples (Harris & Brown, 2010). This implied that the online questionnaire results were generalized to the other students in the Eastern Cape. The online questionnaire had closed and open questions that were simple for the participant to fill in during the data collection process (Phelas et al., 2011). The questionnaire collected Likert-scaled data, which is not easily collected using an interview guide or other qualitative methods. The level of cyber safety awareness among first-year students in the Eastern Cape was collected using a 4-point Likert scale with the following scales to measure the perceptions of the participants: "Strongly Agree" = 1, "Agree" = 2, "Disagree" = 3, and "Strongly Disagree" = 4. In the questionnaire where the questions had a negative implication they were reverse coded implying that "Strongly disagree" =1, "Disagree" =2, "Agree" =3, and "Strongly agree" =4. The questionnaire was divided into five sections. Section A covered the demographic profiles of students, including gender, age, frequency of online activity, and cyber safety involvement. Section B covered the online risks facing the first year in the Eastern Cape. Section C asked the students about their levels of knowledge on different aspects of cyber security aspects. Section C also looked at the effect of cyber knowledge on their level of cyber safety awareness. Section D looked at the effect of cyber safety attitude on the students' cyber awareness level. Section E covered the measures that students viewed as appropriate to deal with the challenges relating to cyber safety awareness faced by first-year students in the Eastern Cape.

Before using the online questionnaire to collect data, they were pre-tested. According to Phelas et al. (2011), pilot testing involves selecting a small number of participants to conduct trials of research instruments before the actual study is done. The piloting of instruments helped identify problem questions and determine the time required to carry out the study. The identified challenges can be adjusted before the actual study is carried out. However, people used in the pilot study were not to be used in the actual study to reduce bias through prior knowledge of the study gained through piloting. The questionnaires were tested on a sample of non-first-year students. Through the pilot survey, there was a refinement of the questions in the questionnaire. Difficult questions were modified so respondents could understand and answer the questions during the survey. The research instruments had subsections based on the research scales presented in Table 5.1. From the literature, the researcher found several thresholds that the scale items reach and are reliable and consistent. In the actual study, any variables below the set alpha = 0.70 were supposed to be dropped from further analysis as they would introduce unreliable results into the study.

Table 5.1: Reliability of scale items

Variable	**indicator**	**loading**	**Cronbach's alpha**	**Source**
Online risk			0.78	(Alzubaidi, 2021)
Cyber safety attitude			0.713	(Chandarman & van Niekerk, 2017)
Cyber safety knowledge	SEA1	0.699		(Matyokurehwa et al., 2020)
	SEA2	0.868		(Matyokurehwa et al., 2020)
	SEA3	0.667		(Matyokurehwa et al., 2020)
	SEA4	0.893		(Matyokurehwa et al., 2020)
	SEA5	0.767		(Matyokurehwa et al., 2020)
	SEA6	0.783		(Matyokurehwa et al., 2020)
	SEA7	0.824	0.791	(Matyokurehwa et al., 2020)
	CSA1_10	0.7152		(Muhirwe & White, 2016)
	CSA1_3	0.6301		(Muhirwe & White, 2016)
Cyber security awareness	CSA1_4	0.6167		(Muhirwe & White, 2016)
	CSA1_5	0.6054		(Muhirwe & White, 2016)
	CSA1_6	0.4251		(Muhirwe & White, 2016)
	CSA1_7	0.4762		(Muhirwe & White, 2016)
	CSA1_8	0.6191		(Muhirwe & White, 2016)
	CSA1_9	0.6828	0.9	(Muhirwe & White, 2016)

The researcher tool constructs from pre-existing questionnaires they were tested and used in published literature with Cronbach alphas ranging from 0.713 to 0.90. This means that the constructs selected were deemed reliable. Therefore, the researcher adopted the constructs to increase transparency and demonstrate that the questions were selected based on a sound rationale. This was used in order to increase the credibility of the study and enhance the trustworthiness of the data collected. The use of pre-existing questions meant that each question can help to avoid bias in the selection process. By providing a clear rationale, researchers can ensure that the questions are not biased towards a particular perspective or outcome. The use of pre-existing questionnaires ensured that the study can be replicated in the future and also ensured that the questions were consistent across studies and that the data collected is comparable. The elements used here were intended to test the significant effect of online risk, cyber safety attitude, cyber safety knowledge and awareness would affect the cyber safety of the university students. The direction and significance of the variables from the previous studies were used as points of comparison between the current study and the previous studies.

5.6.2.2 Expert reviews

Expert reviews are, by definition, the collection of views from people who are knowledgeable in a particular subject (Sanusi et al., 2021). Expert reviews are a research method that involves asking subject matter experts to evaluate a product, service, or idea based on their professional knowledge and expertise subject (Sanusi et al., 2021). The study used expert reviews to examine the critical success factors needed for developing the cyber safety framework for university students in the Eastern Cape. This study's experts were regarded as people with relevant educational backgrounds and experience. Specifically, the experts, in this case, were people with a background in information systems or computer science who had experience in cyber safety awareness. The qualifications and expertise of the experts are described in Table 5.2. The questions which guided the expert review to collect qualitative data is added to this thesis as Appendix 7.

Six experts were selected based on their willingness to participate, having sufficient time to participate, and having effective communication skills. Thus, the experts were asked to review the critical success factors for developing cyber safety awareness among students and the developed framework for cyber safety awareness. The feedback from the experts was

used to refine the final version of the critical success factors and the framework for cyber safety awareness. The researcher made use of thematic analysis to determine the themes which emerged on the critical success factors for cyber safety awareness for first university students. Thematic analysis is a qualitative research method that involves identifying and analysing patterns or themes within data. In the context of expert reviews, thematic analysis can be used to identify common themes or patterns in the evaluation criteria or key themes identified by the experts. The researcher identified potential themes that emerged from the data and provided a clear and concise description of its meaning. In the current study, thematic analysis was also used to identify areas for improvement or to generate new ideas for the development of the final cyber safety awareness model. Expert reviews were used to modify the different versions of the cyber safety awareness framework developed by the researcher. Data from the expert panel was used to firstly review and identify the critical success factors to be used in the development of the cyber safety framework. The expert panels were used to review the developed framework which was developed from Figure 4.3. With the modifications done on the critical success factors and the Figure 4.3 led to the framework presented in Figure 7.2.

Table 5.2: Qualifications and area of specialization of experts used for review

Expert number	Highest qualification	Specific expertise
Expert 1	PhD Computer Science	Academic (Computer programming)
Expert 2	MSc Information Systems	Academic (Networking)
Expert 3	MSc Computer Science	Systems administrator
Expert 4	PhD Information Systems	Academic (Cyber security)
Expert 5	MSc Information Systems	Network systems design and application
Expert 6	B.Tech Computer Science	Cyber Security

5.7 Evaluation criteria

5.7.1 Evaluation criteria for quantitative data

The research was quantitative, so the evaluation criteria adopted were suitable for quantitative research. The pragmatism research paradigm was used, and the evaluation criteria adopted were relevant for such a research paradigm. The elements involved were validity, objectivity, reliability, and internal and external validity (Bhattacherjee, 2012; Oates, 2006).

- *Objectivity* for this study was achieved through other published materials and by using already existing frameworks, theories, and models. The frameworks, theories, and models should have been applied to contexts similar to the one used in the study.

- *Validity* was based on the belief that the data collected from the research participants were trustworthy. In this case, validity was determined by the data collected from students using online questionnaires and expert reviews. The triangulation process meant that data from online questionnaires, literature reviews and expert reviews was used to compare the findings from the different sources to ensure that there was consistency and credibility of the results from the study. This meant that there was a reduction in the extent to which bias was allowed into the study. Triangulation allowed to make inferences from data collected from online questionnaires and expert reviews which could not have been done when using the instruments single handedly.

- Furthermore, internal consistency of the questionnaire items was tested (e.g., using Cronbach's alpha), and convergent feedback from different experts helped refine the tool, enhancing both reliability and validity.

- The *reliability* of the study started with testing the reliability of the research instrument used in data collection. In this case, the reliability of the online questionnaire was tested using Cronbach's alpha. The item construct was deemed reliable if the alpha value was more significant than 0.70. The research was considered reliable when the findings were consistent with other studies tested under

the same conditions. The research findings were compared during the discussion of the results, and areas of similarity and dissimilarity were noted. Additionally, besides from the Cronbach's alpha, there was convergence of feedback from the expert reviews, online questionnaires and findings from previous studies enhancing reliability of the findings from the study. Thus, through triangulation, there was use of data from online questionnaires, expert reviews and literature reviews which was meant to reduce errors and bias being introduced in the study. The process of triangulation increased the consistency, dependability and accountability based on the data collected and the research findings.

- *Internal validity* was regarded as the ability of the research instrument to measure what it was intended to measure by the researcher. In other words, internal validity is achieved when data is collected from different sources linked to the research.

- The *external validity* of the research findings was the data's ability to have generalizations across people, settings, and times. This implied that there were generalizations of the research results from the sample to the population, other people, or organizations (Bhattacherjee, 2012). For the study, external validity will be achieved by generalising the critical success factors and the cyber safety framework to other universities with similar characteristics, such as those in the Eastern Cape.

5.7.2 Evaluation criteria for expert reviews

The validity of qualitative data was determined through credibility, dependability, conformability, transferability and authenticity.

- *Credibility* can be achieved through various means, including the use of rigorous research methods, transparency in the research process, and the use of appropriate data analysis techniques (Bhattacherjee, 2012). Thematic analysis was used to analyse data from expert reviews and the steps which were used in sampling the experts based on their knowledge in computer science and information systems have been outlined. Thematic analysis used in the study is regarded as transparent, replicable, and well-documented. The findings of the results especially on critical success factors have been validated basing on the findings from literature chapters and also the online questionnaires. The proposed critical success factors and models were also peer reviewed by experts thereby providing feedback, quality and rigour which also validates the findings.

- *Dependability* is a crucial element for establishing trustworthiness in research, as it ensures that the findings are reliable, consistent, and can be replicated (Cooper and Schindler, 2014). Researchers strive to verify the consistency between their findings and the original data collected. This means that if other researchers were to review the data, they would arrive at similar interpretations, conclusions, and findings, reinforcing the validity and credibility of the research. The expert reviews were used to interpret the critical success factors and the different stages of the cyber safety framework.

- *Conformability* in research refers to the level of objectivity, where the congruence between multiple independent individuals regarding the accuracy, relevance, or meaning of the data can be determined (Cooper and Schindler, 2014). On the other hand, transferability refers to the potential for the findings to be extrapolated or generalized to other settings or contexts beyond the original research setting. In this case the data collected using expert reviews was tested for congruency with data from online questionnaires and review of literature which meant that the data can have some of generalisations with first year university students in the same context as the ones used in the study.

- *Transferability* in qualitative research refers to the extent to which the research findings can be applied or transferred to contexts beyond the scope of the study (Oates, 2006). In essence, transferability suggests that the results of the research can be relevant and useful in similar situations or for other individuals. In this case it refers to the extent in which the research findings can be relevant to university students in similar circumstances as the ones used in the study.

- *Authenticity* in research refers to the extent to which researchers are able to capture the diverse perspectives and values of participants in their study and promote change across both individuals and systems during the analysis phase (Bhattacherjee, 2012). The research can be regarded as authentic as it intends to promote change in cyber safety awareness among the first year university students.

5.8 Ethical considerations

Ethics are the moral considerations that distinguish between the good and the bad (Bhattacherjee, 2012). Ethics are necessary for research to guard against manipulation by people or organisations to advance their agenda at the expense of the research subjects, which falls against the expectation of scientific conduct. The researcher made sure that the study complied with the ethical principles of the University X's Research Ethics Council, which meant that the researcher's application for an ethical clearance must be cleared before the researcher begins data collection. The University X's Research Ethics Council approved the study with the following certificate reference number: PID011SMAK01. The permission to carry out research is attached as Appendix 2, and the ethical clearance is attached as Appendix 3. Permission was also granted to collect data from University Y's students. The participant's agreement to participate in the study was explained on the top portion of the online questionnaire, which also included the study's purpose. Confidentiality and anonymity were assuredly preserved, and the researcher clarified that the study was academic. The researcher made sure that the research was anonymous, as there was no collection of personal information from the students. The students were informed of their right to withdraw at any point during the data collection process without any consequences. The collected data was stored separately from the data used for analysis, and access was restricted to the researcher and the supervisors when needed.

5.9 Data analysis method

5.9.1 Data analysis for online questionnaires

Cronbach's alpha was used to test the reliability of the questionnaire instrument, specifically the individual scale items. The students' perceptions were measured using a 4-point Likert scale, and frequencies and percentages were used to determine the dominant answer. Descriptive statistics of mean and standard deviation were used to determine the spread of the student's responses. The relationship between online frequency, online behaviour, cyber safety attitude, cyber safety knowledge, and cyber safety awareness was analysed using the Chi-square test in the Statistical Package for the Social Sciences (SPSS version 28). In SPSS, the Chi-square test was put under the function non-parametric tests, which fit the data type that was not numerical and did not follow a normal distribution. Alternatively, the same test can be calculated using the cross tab function in SPSS, in which the expected and observed

functions need to be selected, and this allows the software to calculate the number of observations for the given cell, as well as the expected number of observations for a given cell. The Chi-square test is based on the following equation:

$$\chi^2 = \sum\left(\frac{O-E}{E}\right)^2 \quad \text{Equation 1}$$

where χ^2 is the test statistic, $\sum$=the sum of O, the observed frequencies and E expected frequencies.

Degrees of freedom (df)=(rows-1)x (columns -1)……..Equation 2

Since the contingency tables and degrees were automatically calculated in SPSS, there was no need to use the Chi-square tables to determine the significance levels. Significant associations between the variables under study were noted if $p<0.05$. From the significance based on the p-values of the Chi-square tests, a decision or a conclusion on the hypotheses formulated in Chapter 1 was made. For example, suppose a p-value from the SPSS output was 0.01. In that case, it is below the set threshold of 0.05, which would show that there was a significant association between the variables being tested. This would lead the researcher to reject the null hypothesis that there was no significant association between the variables being tested. In this case, the researcher will be made to accept the alternative hypothesis.

5.9.2 Data analysis from expert interviews

The study collected qualitative data using expert reviews which was analysed using thematic analysis especially on the critical success factors which affect cyber safety awareness of the university students. In the context of expert reviews, thematic analysis can be used to identify common themes or patterns in the evaluation criteria or key themes identified by the experts. The researcher identified potential themes that emerged from the data and provided a clear and concise description of its meaning. In the current study, thematic analysis was also used to identify areas for improvement or to generate new ideas for the development of the final cyber safety awareness model. Expert reviews were used to modify the different versions of the cyber safety awareness framework developed by the researcher. The experts were also used to give feedback on the proposed cyber safety awareness framework for first year university students. The feedback from expert reviews was validated based on theories and literature reviewed in Chapters 2, 3, and 4. The input from the experts was checked to see if it

was aligned with the variables aligned with the study's objectives, for example, cyber safety attitude, online risks and cyber safety awareness. If the reviewers' feedback were not in line with the objectives, the feedback was disregarded as it was irrelevant in determining the critical success factors.

5.10 Summary

The chapter dealt with how the research was conducted to collect data to answer the study's main objective. The chapter presented the research methodology which was used in this study. Following the research methodology, the chapter addressed the pragmatism paradigm and its advantages in terms of the detachment of the researcher from the participants, which meant that data was independently collected. The research paradigm also influenced the research design for the study and how data was collected and analysed. A quantitative research design was selected for the study. In the chapter, there was coverage of the population and sampling procedure. The sample size calculator was used to determine the number of participants who participated in the study. Online questionnaires were described, and the kind of data to be collected was also described and explained. The use of expert reviews in determining the critical success factors and the proposed model was discussed in the chapter. The ethical considerations which were observed in the study were also discussed. The ethical clearance number was listed, and its appropriate section in the appendices was cited. The data analysis procedures were also presented, and the relevant formula was shown.

The chapter was central in developing the cyber safety framework in that it facilitated the collection and analysis of data. Results from the questionnaires were important in that they were inputs in developing the initial models, identifying the critical success factors, and the final model. The reviews from the experts improved the initial models, critical success factors, and the cyber safety framework.

The next chapter presents analyses and discusses the research findings of the study. The chapter covers the analysis of the results and how the findings are situated in the global literature. The conclusions on the hypotheses were also made in the chapter.

CHAPTER 6

DATA ANALYSIS AND INTERPRETATIONS

6.1 Introduction

The previous chapter dealt with the research methodology that guided this study, which included the research methodology, research paradigm, research, and data collection instruments. The researcher collected primary data using online questionnaires and expert reviews to meet the study's objectives. Primary data was augmented by secondary data, which came from already existing literature.

The study aimed to develop a cyber safety framework for first-year university students at selected universities in South Africa. The chapter presented the results following the study's research objectives formulated in chapter 1. In the chapter, there was the testing of the hypotheses for the study, and conclusions on the null and alternate hypotheses were made.

This chapter details data presentation, analysis, interpretation, and discussion. The chapter analyses and discusses the research findings based on data from first-year university students from the University X and University Y. The study aimed to develop a framework for cyber safety awareness amongst first-year students in the Eastern Cape, South Africa. The researcher focused on first-year students from different faculties across the two universities. Data were analyzed using Statistical Package for Social Sciences (SPSS) and MS Excel for better tables and graphs. Data were analysed using descriptive statistics such as mean, standard deviation, frequencies, and percentages to determine university students' perceptions. The level of association between the variables was tested using Chi-square tests, and significance was deemed when $p<0.05$. The reliability of the research instrument was tested using Cronbach’s alpha test.

The discussion of the findings was based on the literature reviewed in chapters 2, 3, and 4. The discussion also highlighted the areas of agreement and disagreement with the study results compared with the existing literature. The chapter also used the theory of planned behaviour and social learning theory to discuss the research findings. From the discussion of the results, it is clear that dominant factors will be used to develop a cyber safety framework to reduce the online risks students face for social and academic reasons.

6.2 The online questionnaire

The research used an online questionnaire to collect primary data from university students at University X and University Y. The instrument was developed based on the literature reviewed in the second chapter, and some elements were taken from the Theory of Planned Behaviour (TPB). The instrument was developed in Survey Monkey, and the MS Word version of the questionnaire is attached as Appendix 1. The questionnaire was predominantly close-ended for easy coding and analysis and had very limited options for students to select other options than the ones to which the researcher restricted them. The online questionnaire was divided into Section A, which covered the demographic background of the students as well as their online frequency, and experience in working with smartphones. Section B covered the online risks, and Section C covered the knowledge about cyber threats and how it affects cyber safety awareness. Section D detailed the effects of cyber attitudes towards cyber safety awareness. Section E looked at the measures that can be used to minimize the challenges faced by students when they are online. From sections B to E, most of the questions were put on a 4-point Likert Scale which ranged from 1 Strongly agree to 4 Strongly disagree. In the questionnaire where the questions had a negative implication they were reverse coded implying that "Strongly disagree" =1, "Disagree" =2, "Agree" =3, and "Strongly agree" =4. The findings of reverse coded questions were presented in Table 6.8 and caption was made to that effect such that the interpretation of the results was not misunderstood.

Before the final questionnaire was distributed to the students, the research team conducted a pilot study in which a pre-test of the instrument was done. This was done with students who were not first-years at University X. The pre-test aimed to remove or modify unclear questions. More so, the aim was to determine the time needed to complete the questionnaire. Thus, the feedback from the non-first-year students was used to modify the final version of the online questionnaire. In addition, the use of non-first-year students was intended to remove bias in answering the questionnaire based on the pre-existing knowledge they would have gained.

6.3 Response rate

Based on the sample size calculator, the sample size for the study was 353 students. However, the researcher distributed as many links as possible to the students, hoping that if

others did not respond, there would be others who would. In this case, the researcher received 383, the target sample for the study, of 450 online questionnaires. This means that there is an 85% response rate (Table 6.1). The high response rate meant increased confidence for the researcher to start the data analysis process as there was non-bias of the collected data and representativeness of the collected responses.

Table 6.1: Response rate

Instrument	Instruments distributed	Number returned	Response rate (%)
Online questionnaires	450	383	85%

6.3.1 Reliability of questionnaire scale items

Table 6.2 tests the reliability of the scale items of the online questionnaire used to collect data from university students. Cronbach's alpha was used to determine the level of reliability of the scale items of the online questionnaire. Cyber safety knowledge and measures to deal with cyber safety challenges had Cronbach alpha values above 0.70, which meant that the measurements from the scale items were reliable. However, the effects of knowledge on cyber safety and attitude towards cyber security had Cronbach alpha values below 0.70, which meant that the measured scale items were unreliable. Overall, it is noted that the questionnaire had an alpha value of 0.77, which meant that there was internal consistency with the measuring instrument.

Table 6.2: Reliability of questionnaire scale items

Scale	Cronbach's alpha	Number of items
Cyber safety knowledge	0.781	7
Effects of knowledge on cyber safety	0.534	7
Attitude towards cyber safety	0.603	5
Measures to deal with cyber safety challenges	0.794	6
Overall	0.772	25

6.4 Demographic profile of the respondents

6.4.1 Age of respondents

The results in Table 6.3 show the age of the respondents used in the study. From the table, it can be noted that the majority of the respondents were in the 18–24 age group. The findings are not surprising, as this is the age group in which students are expected to begin their university education. The least respondents came from those between 35-44 years (14%). The results reflect that at any age, anyone can join the university. More specifically, there was a

need to look at the student's age, as age is expected to affect the amount of time one spends online and ultimately bring awareness to the issue of cyber safety. The dominant age group for the study was almost similar to a study in Zimbabwe by Matyokurehwa et al. (2021), in which 87% of the university students came from a 16-26 year age group, which is similar to the age range used in the study. More so, the age ranges of this study were lower than that for students from Hungary in the age range 20–30 was considerably higher. However, they were within the age range of university students from South Africa (Cranfield et al., 2021).

Table 6.3: Age of respondents

Age group	Frequency of Respondents	Percentage of Respondents
18-24	317	82
25-34	52	14
35-44	14	4

6.4.2 Gender of respondents

The results presented in Figure 6.1 show the gender of the respondents. The results have shown that the majority were females, which accounted for 65%. Males accounted for 35% of the respondents. Overall, it can be stated that there was a gender imbalance among the respondents used in the study. However, the imbalance is difficult to control since it is online-based, and at the same time, this also points out that more females than males have been accepted into universities. At the same time, the research will be interested in determining how gender influences perceptions of online risk.

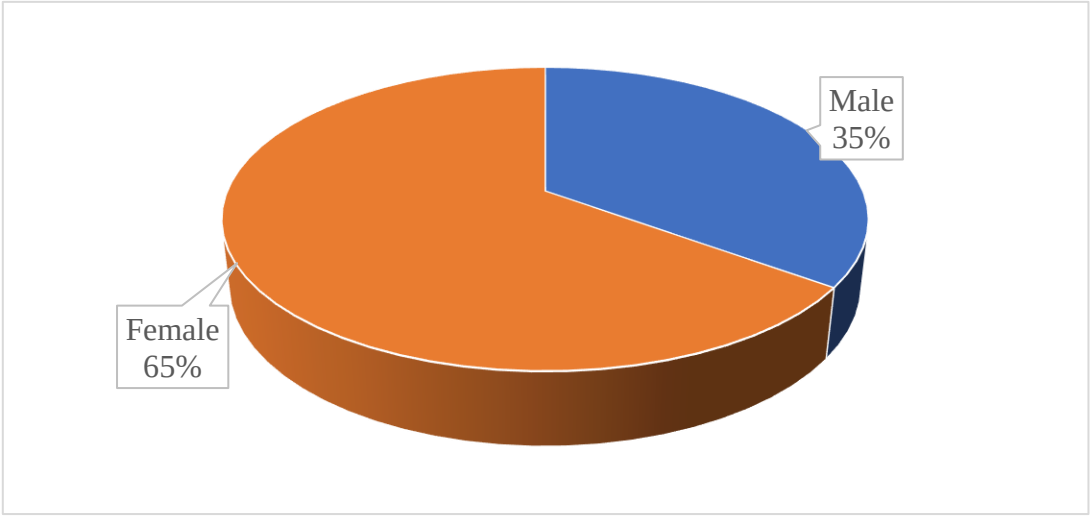


Figure 6.1: Gender of respondents

6.4.3 Years using a computer or a smartphone

The results presented in Figure 6.2 show the years in which first-year university students have been using a computer or a smartphone. Most students (33%) indicated that they had been using a computer or smartphone for the last 3–5 years. Some 25% of the students used in the study indicated that they had used a computer or a smartphone for about 6-9 years. About 22% of the students also indicated that they have been using a computer or smartphone for more than ten years. Overall, it can be noted that all the students used in the study have been using electronic gadgets for some time. This implies that they have been using these gadgets online, which means they know the risks they face online.

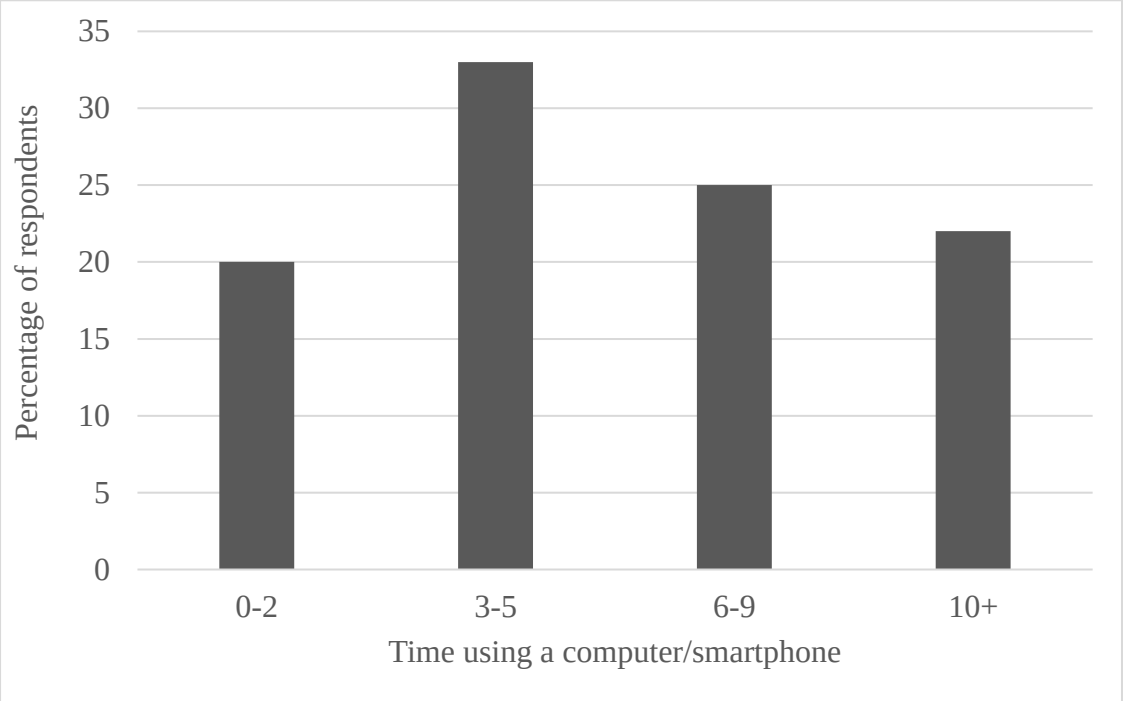


Figure 6.2: Time using a computer/smartphone

6.5 Online risks facing first-year students at a selected university in Eastern Cape

To answer this objective, there was a need to determine the online frequency of first-year university students. This can infer students' exposure risk based on the frequency. It is believed that the longer someone stays online, the greater the risk of cyber threats.

6.5.1 Online frequency of the university students

For this question, students were asked to estimate how much time they spent online. The frequency ranged from once a week to every hour (Table 6.4). However, the frequency of being online may have been affected by adopting online and blended learning during and after the COVID-19 pandemic.

Table 6.4: Frequency of online activity by university students

Online frequency	Frequency of Respondents	Percentage of Respondents
Every hour	240	63
Half a day	116	31
Once a week	5	1
After work	5	1
Others	14	4

Results presented in Table 6.4 show that most of the students (63%) are always online every hour, and 31% of the students are also available for most half of the day. Very few respondents also indicated that they are online once a week after work. Thus, it can be noted that most students have a high frequency of being online.

6.5.2 Online risks faced by first-year university students

Figure 6.3 shows the different online risks first-year university students face in the Eastern Cape. Results indicated that 39% of the students were exposed to cyberbullying. The other common risk for university students was phishing scams (22%). Some students showed risks such as identity fraud (17%). Students faced online risks such as invitations to pornography (13%). Sexting was the least form of online risk that the students faced. From the results, it can be deduced that the students faced various risks while engaged in online activities. The students were mostly online, exposing them to cyber-space risks.

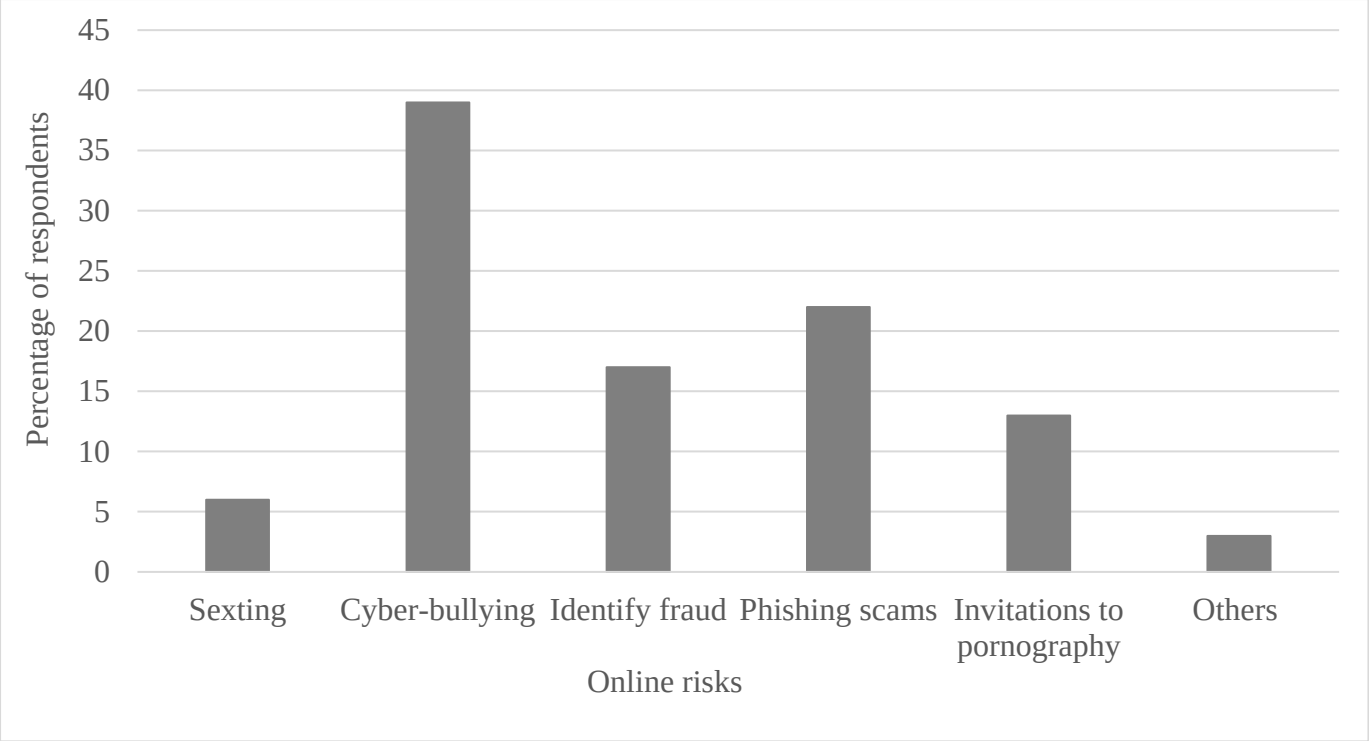


Figure 6.3: Online risks faced by first-year university students

In the first chapter, the researcher tested the hypothesis that there is no significant association between the time spent and the online risks faced by first-year students at selected universities in the Eastern Cape. A Chi-square test was used to determine if there is a significant association between the time spent online and the online risks faced by the students. Results presented in table 6.5 show that there is a significant association between the gendered nature of the student and the risk faced ($\chi 2=567$, $p=0.000$). The p-value is less than the set threshold of 0.05, and as such, we do not accept the null hypothesis that there is no association between the stated variables.

Table 6.5: Chi-square test for association between online frequency and online risks faced by students

	Value	df	Asymp. Sig. (2-sided)
Chi-Square	566.752	4	.000

The results show that the time one uses while online affects the likelihood of facing online risks. Thus, the more time the student spends online, the higher the risk of facing online threats. Thus, the researcher restates the hypothesis for this objective: *There is a significant association between time spent online and online risks faced by first-year students at selected universities in the Eastern Cape.*

Discussion of findings

The study results showed that most students spent most of their time in online classes. This is probably because, due to the COVID-19 pandemic, the shift from physical classes to online and blended learning increased students' online presence. This is supported by UNICEF (2020), which stated that as a result of the COVID-19 pandemic, the closure of universities globally and in South Africa implied that there was an increase in internet usage by 50% (UNICEF, 2020). The use of blended learning meant that students spent more time online, which increased the probability of the students being exposed to challenges associated with over-access to online technologies (Dhawan, 2020). According to Zahidah et al., (2020), the more one spends online, the higher the likelihood of facing online threats. Moreso, there is a psychological need for one to remain connected online due to several reasons, which further makes the end user more exposed to online risks (Quayyum et al., 2021).

The results of this study showed that the dominant online risks that the students faced were cyberbullying, phishing scams, and identity theft. Other less common forms of risk were invitations to pornography and sexting. The study results are the same as those from Malaysia by Zahidah et al., (2020), who indicated that there are too many unknown risks and threats in different forms that students expose themselves to online. The exposure of university students to online risks worsened due to the COVID-19 pandemic, which made universities globally and in South Africa adopt online learning. When the pandemic receded, face-to-face and online learning (blended learning) were adopted. More so, the vulnerability of university students is further worsened by the fact that universities leave their networks open to allow students and staff to access services on and off campus (Matyokurehwa et al., 2021). The results of the study were similar to those of Beverley and Covey, (2018); Paluckaitė and Žardeckaitė-Matulaitienė (2016), who found that the common online risks were cyberbullying, sexting, and communication with strangers, sending embarrassing photos. Similar online risks, such as identity theft, illegal downloading, and pornography, were found to be less prevalent in this study. Still, the same findings were reported by Al-Badi et al. (2016) and Schilder et al. (2016). However, Wang and Alexander (2021) found other forms of online risks that were dominant during the COVID-19 pandemic. The common risks faced by students were spam mail, malware, distributed denial of service (DDoS), suspicious websites and domains, and social media messaging. There has been an increase in cyber events as hundreds of institutions and colleges have increased their digital operations. These

incidents range from intrusions into Zoom meetings to phishing efforts targeted at students and professors to more serious data thefts and ransomware assaults (Patrick et al., 2021).

The results of the study indicated several online risks. Still, they did not quantify the frequency of the online risks and threats, which is different from the study in the United Kingdom, which saw a 400% rise in email and phishing attacks among university students during the COVID-19 pandemic (Mpungose, 2020b). In South Africa, KnowBe4, a security awareness training firm, reported a 600% increase in phishing email attacks linked to COVID-19 in the first three months of 2020 (Salami, 2021). This means that COVID-19 increased online risks, particularly from phishing emails containing misinformation about COVID-19. The lack of knowledge on cyber security can be attributed to the lack of training and initiatives to raise cyber security awareness by institutions of higher learning such as universities (Alqahtani, 2022b). This can be done by including cyber security awareness components in the curricula of university students, especially first-year university students.

6.6 The effect of cyber security knowledge on cyber safety awareness among first year students in Eastern Cape

The university's first-year students were asked about their level of knowledge about some elements of cyber safety (Figure 6.4). The responses were rated as "very knowledgeable," implying that the students had advanced knowledge about the aspects in question. The other option was "knowledgeable," which meant they had some idea of the elements of cyber security. Lastly, the other option was that the students "did not know" about the element of cyber security in question. To generalise the findings, very knowledgeable and knowledgeable would be summarized to imply that the students knew. The results showed that most students (55%) did not know what phishing is, while 38% indicated that they knew it. Seven per cent of first-year university students indicated they were very knowledgeable about phishing. Thus, 45% of the students knew about phishing. Overall, it can be noted that most students do not know what phishing is, and as such, with the long periods they spend online, university students are vulnerable to phishing attacks. Most students (52%) indicated they were knowledgeable about anti-virus software, and 10% were very advanced in using it. Some 38% of the students indicated they needed to learn how to use anti-virus software. The bulk (90%) meant they could have their computers protected by using anti-virus software. The students (61%) indicated that they needed to learn how to use a firewall, which means

that they needed to learn about the function of the firewall in protecting the user from threatening traffic from the public internet. The other 39% indicated that they knew about using a firewall.

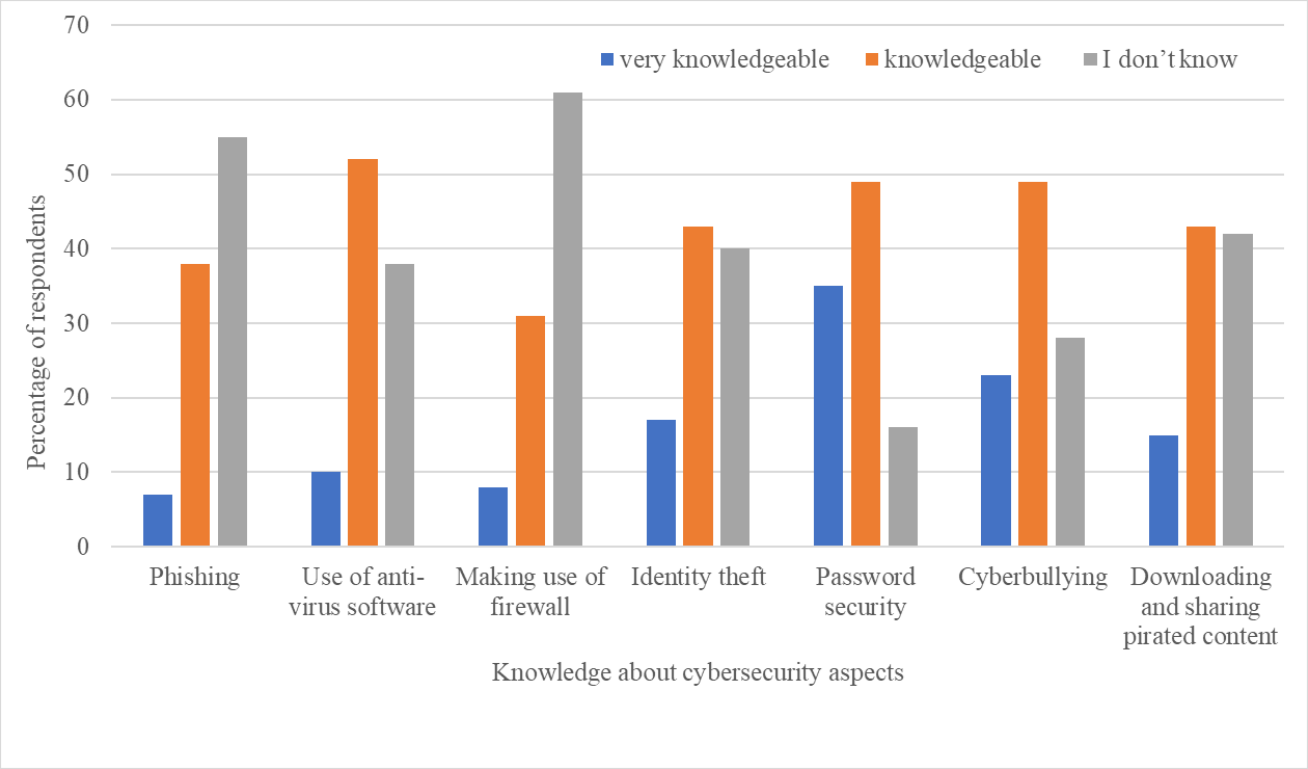


Figure 6.4: Knowledge about cyber security aspects

Results presented in Figure 6.4 showed that 43% knew about identity theft, and 17% were very knowledgeable about it. However, 40% of first-year students needed to learn what identity theft was. The mixed knowledge about identity theft implies that some students could be exposed to identity theft when they provide their identities to unknown individuals in cyberspace. The first-year university students also indicated that they were very knowledgeable about password security (49%), and another 35% indicated that they were very knowledgeable about password security. Thus, 84% of the students had varying knowledge about password security. Some 16% stated that they needed to learn about password security. The lack of knowledge about password security would mean that their gadgets were at risk when they went online. The students indicated that they knew about cyberbullying (49%), and another 23% were very knowledgeable about it. Another 28% indicated that they did not know what cyberbullying is, which may suggest that they can be bullied without knowing it. It was also found that the students knew about downloading and

sharing pirated content (43%), and 15% were very knowledgeable about it. More so, 42% said they did not know about downloading and sharing pirated content. This means that without knowing about downloading and sharing pirated content, they can have their identity stolen in the long run. It is also illegal to download and share pirated content. The students' perceptions were also quantified using a 4-point Lickert scale; the results are presented in Table 6.6. The frequencies and percentages of the Lickert scale data are presented in Appendix 4.

Table 6.6: Effects of cyber safety knowledge on cyber safety awareness of the first year students

Views of the first-year students	Mean	Std. Deviation
I am not ignorant of security concerns regarding smartphones.	1.8596	.61148
I am unaware of all the security risks and necessary security practices.	2.1257	.65342
I never share my password or post it where others can access it.	1.5520	.62221
I know how to protect against ‘social engineering’ ‘phishing’ and ‘cyber-crime’.	2.4023	.78104
I always lock my PC and employ my system’s password-protected screen saver when away.	1.7637	.66416
I am careful when opening email attachments and links.	1.8415	.63674
Valid N (listwise)		

The results presented show the effect of cyber safety knowledge on the cyber safety awareness of the students. The students agreed they were of the security expected of them when using smartphones (mean=1.9; standard deviation=0.61148). This implies that the student knows the security measures they need to implement. Results indicated that the students admit or agree (mean=2.1257) that they are not fully aware of all the security risks and necessary security practices. This is supported by the findings presented in Figure 6.4, which showed that the students had different levels of knowledge about cyber-related aspects. The students also agreed (mean=1.5530, standard deviation=0.6221) that they do not share passwords with anyone. This means they know the risks they have when sharing passwords with people. Results of the study also indicated that the students knew how to protect themselves against threats such as ‘social engineering, ‘phishing’ and ‘cyber-crime’. Results also showed that the students, when away, always lock their PC and employ my system’s password-protected screen saver (mean=1.7, standard deviation=0.66416). Due to the

challenges of phishing, students stated that or were of the view that when opening email links and attachments, they exercised caution.

The results presented in Table 6.7 show the test of a hypothesis on the level of association between cyber security knowledge and cyber safety awareness among first-year students used in the study. The results show a significant association between cyber security knowledge and cyber safety awareness ($\chi 2$=169.605; p=0.000). In this regard, the p-value for the study was below the set value of 0.05, meaning that the researcher failed to accept the null hypothesis, which stated that there is no significant association between cyber security knowledge and cyber safety awareness. In this case, the researcher adopted the alternate hypothesis (H1: There is a significant association between cyber security knowledge and cyber safety awareness among first-year students at selected universities in the Eastern Cape).

Table 6.7: Chi-square test for the association between cyber security knowledge and cyber safety awareness among first year students

	Value	df	Asymp. Sig. (2-sided)
Chi-Square	169.605	2	.000

It can be inferred that the student's knowledge of cyber security makes the student aware of the cyber safety measures that must be taken when faced with online risks. However, as depicted in Figure 6.4, various levels of knowledge range from being very knowledgeable to general knowledge, giving the students different levels of awareness. Thus, the researcher restates the hypothesis for this objective: "There is a significant association between cyber security knowledge and *cyber safety awareness among first-year students at selected universities in the Eastern Cape."*

Discussion of findings

The study results also indicated that some students had less knowledge of online risks. These findings are supported by (Mpungose, 2020b), who indicated that some of the students lacked digital literacy, which is one of the needed skills to navigate the universities' digital technologies. The lack of knowledge in the study can be because there are so many threats and risks the students face when they are online Zahidah et al., (2020); in a study in Malaysia that there are too many unknown risks and threats in different forms to which students expose themselves when online. With specific reference to students, studies in Saudi Arabia, New

Zealand, and Bangladesh indicated that students of various age groups could not identify cyber security terms such as phishing (Alqahtani, 2022b; Gabra et al., 2020a).

With the increased usage of online learning during the COVID-19 pandemic, cybercriminals took advantage of the confusion caused by the spread of the disease. The human being is regarded as the weakest entry point for all cyber activities (Chandarman & van Niekerk, 2017; Matyokurehwa et al., 2021), and there is a need to assess their knowledge of the various online risks. The results of this study showed that the university students used in this study had mixed cyber knowledge and that in itself makes the students develop cyber security awareness. Thus, this implies that they had mixed knowledge about what to do and what not to do on the internet, and the lack of cyber threats makes them easy targets for cyber-attacks (Matyokurehwa et al., 2021). However, despite the students knowing about cyber security, they may not be aware of the digital footprint they live behind on the internet. This view is supported by (Alqahtani, 2022b) in a study on students in the United States, where it was found that students were conscious of their actions. However, they were unaware of their data being used elsewhere within and between university systems. The results are also similar to the study from Nigeria by Alharbi & Tassaddiq (2021b), who found that students had a basic knowledge of cyber security but were unaware of what to do with their knowledge to make themselves secure. As some of the students indicated that they did not know about some of the cyber security aspects, the same was found by Tick et al. (2021), whose previous study from South Africa indicated that mobile phone users are vulnerable to attacks as they are less concerned about their cyber security. Therefore, cyber security knowledge can be used as a launch pad so that university students can be aware of cyber safety measures when engaged in online activities. With that in mind, it is critical to understand their skills and knowledge on aspects such as password use, as they are vulnerable to cyber threats.

The study findings showed that the students knew about some of the online threats, which shows a perception of risk among the students. The findings of the study are supported by Gabra et al., (2020a), who stated that another critical aspect of cyber knowledge is risk management, which implies that the student, whether online, has to develop a perception of risk such that there can be a need to mitigate the perceived risk again. Thus, the perception of risk leads to developing protective behaviour in the technology used. Cyber safety awareness is a good mitigation measure against online attacks that a user can face. The study's findings are supported by Alharbi & Tassaddiq, (2021b), who stated that new cyber threats are coming

up and leading to information loss and misuse. The main targets are universities, where students interact, and data breaches occur due to a lack of awareness and the consequences of online sharing of personal information. More so, the study's findings are also in line with Rajan (2010), who found out that people still fell victim to phishing despite knowing about it. However, the chief reason was incorrect behaviour patterns towards online security.

The study's findings stated a significant association between knowledge of cyber threats and cyber safety awareness. The results are similar to a cross-country study in Turkey, Israel, Poland, and Slovenia in which correlations were found between mindfulness, understanding, and activities in which protection tools were used (Alqahtani, 2022b). However, the high levels of knowledge were found not to be used, which translates to the fact that knowledge of cyber threats does not translate to cyber security, safety, or awareness. However, students with insufficient knowledge would be easily deceived by the different threats.

6.7 Effect of cyber security attitude on cyber safety awareness of first year students in Eastern Cape

The results presented in Table 6.8 are from 4-point Lickert scale data, the Lickert scale data was reversed as the questions and the scales ranged from 4= Strongly disagree, 2= Disagree, 3= Agree, and 4= Strongly agree. In this case, the results were averaged to produce the mean answer. The standard deviation was used to determine the extent to which answers were spread from the mean answer. The lower the standard deviation, the lower the variability in the spread of the answers. The frequencies and percentages of the Lickert scale data are presented in Appendix 5.

Table 6.8: Effect of attitude on cyber safety awareness of first year students

Views of the first-year students	Mean	Std. Deviation
Changing passwords is a waste of time because you can still get hacked.	2.4543	.85423
It is too difficult to remember passwords; therefore, I use my name or something easy to remember.	2.1199	.83712
Posting pictures and bad messages online about my college students makes it anonymous and is much better than saying it to their faces.	2.9399	.96914
The security settings and tools slow me down and are pesky. I turn them off or disable them.	2.6624	.73744
Updating my security software and Windows /Apple is too time-consuming, annoying, and uses up my bandwidth/ data bundle.	2.6006	.82981

The study results indicated that students disagreed (mean = 2.45) that changing passwords is a waste of time because you can still get hacked. The low standard deviation of 0.85 shows less variation in the answers. This means that the students saw that they did not waste time when they change the password of their computers even though they can be hacked. The results also indicated that the students disagreed (mean = 2.12, standard deviation =.83712) that it is too difficult to remember complex passwords; therefore, I use my name or something easy to remember. This shows that the students have a good attitude towards their online security and reduce their vulnerability towards online challenges. The students disagreed (mean = 2.94) that posting pictures and bad messages online about my college students makes it anonymous and is much better than saying it to their faces. It shows that the students were aware that sharing pictures and messages online was a bad online practice.

Moreover, the students disagreed (mean=2.66) with the view that the security settings and tools slow me down and are pesky. I turn them off or disable them. Thus, it can be inferred that students use the security settings on their phones, tablets, and computer gadgets when going online. This implies that they have a good attitude towards cyber safety awareness and increase security online. The study results indicated that the students disagreed (mean = 2.60) with the view that updating security software and Windows/Apple is too time-consuming, annoying, and uses up my bandwidth/data bundle. From the statement mentioned above, it can be noted that students were not worried about the time that electronic gadgets took to update and data costs.

Table 6.9: The level of association between cyber security attitude on cyber safety awareness

	Value	df	Asymp. Sig. (2-sided)
Chi-Square	57.966	2	.000

The results presented in Table 6.9 show the Chi-square test results for the association between cyber security attitude and cyber safety awareness. ($\chi 2$=57.966, p=0.000). The result shows a significant association between cyber security attitudes and cyber safety awareness. From this study, it can be deduced that the students' attitudes towards cyber security would be associated with the cyber safety awareness of the students. Since the p-value from this study was less than the set p-value of 0.05, the researcher fails to accept the null hypothesis: "There is no significant association between cyber security attitude on cyber safety awareness of first-year students at selected universities in the Eastern Cape." The alternative hypothesis is

that: *There is a significant association between cyber security attitudes on cyber safety awareness among first-year students at selected universities in the Eastern Cape.*

Discussion of findings

The findings of the study indicated that the students have knowledge and experience of safety issues to be engaged when online, and the results of the study are supported by Vafaei-Zadeh et al. (2019), who stated that individual experiences and knowledge affect the attitude of an individual, especially in the context of information security awareness. In this regard, some students indicated that they are aware of the various threats and that in itself is a driver of attitude, as it is anticipated that users will take security precautions. The Theory of Planned Behavior, which proposes that information security knowledge impacts the attitude toward having greater intention about employing protection measures such as anti-malware software, unique passwords, and firewalls, is then used to corroborate the study's findings.

The study results indicated that the students are concerned about their security, shown through password strength and the need to change them often. This contradicts Matyokurehwa et al., (2021), who indicated that students have more time on the internet and are not concerned about their identities and passwords. Thus, the students used in the study have a protective attitude by refraining from using weak passwords and are on the lookout for suspicious links, which is also supported by Chigada & Madzinga, (2021b). Since students believe they will understand the digital environment better with age and experience, the concern about their online safety implies that this will impact their online behaviour. However, it is not entirely clear whether a critical understanding of the digital environment leads to cautious behaviour regarding personal data protection. There is a misconception that one will be protecting oneself with a unique password, and there is no need to worry about other cyber security threats (Hunt, 2016). Although it’s a significant good step to create unique passwords, it is not enough to keep the user's information private due to hackers having knowledge and technologies which can decrypt passwords or do a password bypass (Hunt, 2016).

The study's findings showed that the level of cyber security influenced university students' cyber safety knowledge. The findings might be addressed in relation to Ajzen's (1991) theory of planned behaviour, which claimed that a person's attitude toward behaviour and their

perception of behavioural control impacts their intention to engage in the behaviour under consideration. In this case, some students had a different attitude towards cyber safety, so their likelihood of doing the same risky behaviour was high. In some cases, it can be assumed that the level of knowledge about online risk would lead to cautious behaviour regarding personal data protection, although there is uneven digital literacy. The need to look at the safety of the students emanates from the view that there are changes in attitude, behaviour, and perception brought about by the changes in technology (Laher et al., 2021b). This was the case when the shift to online technology was introduced due to the COVID-19 pandemic, with the understanding that if they decide not to share the information. Thus, such beliefs make young people do whatever they want on the internet, believing that others do not see what they do online. Whether harmful or healthy, situations like online behaviour need collaboration across several spheres of judgment. Information from the social and moral domains will be utilized to direct young people in decision-making based on the cumulative interpretation of prior encounters within social situations. A teenager weighs information from social and moral realms when determining what to do in situations that call for moral judgment, whether online or on a mobile device. This becomes clear when examining how young children may behave differently in comparable circumstances or how moral ideas vary across cultures. More so, as the students have just shifted from being children, there is also a change from compliance and commitment to the parents toward peer orientation (Wang & Alexander, 2021b), and this influences the decisions that they reach towards online behaviour, risk perception and attitude towards cyber security and awareness.

The study's findings revealed that the participants did not share the belief that criticizing college students anonymously and online was preferable to confronting them. The same outcomes were discovered for students in Silicon Valley, where surveillance of their actions did not change their understanding of the security of the information they provided (Alqahtani, 2022b). Behaviour change can be made through training to ensure students improve their understanding of cyber safety and threats. However, there is a need to combine awareness, attitude, and knowledge to promote secure online behaviour among university students. Therefore, the factors studied in this study cannot be used in isolation for improved cyber safety awareness.

According to the study, students did not believe that criticizing college classmates in person was preferable to posting derogatory images and remarks online since it was anonymous. The

results point to the fact that the students may post even good pictures without knowing that whatever they share on social media will be shared without their consent. This lack of knowledge needs to be addressed so that the students know about the risks of the things and content they share online. This is supported by Lester (2019), who stated that students are not aware that sharing pictures on sites like Snapchat is not as safe as it may appear because the photos will be the property of Snapchat, which can share them without the consent of the student who would have uploaded them.

6.8 Measures that can be put to protect students from cyber attacks

The results, presented in Table 6.10, show the measures the students can use to protect against cyber-attacks. Results of the study have shown that the students agreed (mean = 1.64) that they need training programs to protect themselves from cyber-attacks, although some have shown that they have less knowledge of cyber security (Figure 6.4). The frequencies and percentages of the Lickert scale data are presented in Appendix 6.

Table 6.10: Measures that can be put in to protect students from cyber attacks

	Mean	Std. Deviation
Training and awareness campaigns	1.6393	.59694
Frequently change secure password changes	1.9704	.73285
Practising safe computing	1.6412	.57518
Incorporate cyber security issues in the curriculum	1.9178	.63179
Gaming for cyber security awareness	1.9934	.69298
Development of cyber security policy or framework	1.8245	.61998
Valid N (listwise)		

Since there was a standard deviation of .83712 when the students were asked about their view of frequently changing passwords, it showed that there were divergent views about the item in question. Thus, some students indicated they need to frequently secure password changes, and most agreed (mean = 1.97). The students also agreed that they must practice safe computing to protect themselves from cyber-attacks. Students agreed (mean = 1.91) that cyber security issues should be included in the curriculum so that they will know how to protect themselves against cyber-attacks and possibly implement what they have learned from the university curriculum. The results also showed that gaming in cyber security could be another way to protect students from cyber-attacks. The findings indicated that the university students agreed (mean = 1.82) with the view that there is a need for the

development of a cyber security policy or framework that can be followed by the university or communities such that there is a reduction in the cases of cyber-attacks among university students.

Discussion of findings

The study results indicated that the measures to be used to protect the students from cyberattacks would be to train them to use online technologies, especially after the introduction of online learning. The results are supported by Hedding, Greve, Breetzke, Nel, & van Vuuren, (2020) and Tick et al., (2021b), who indicated that the adoption of online teaching by universities across the world was done without the students and the lecturers being trained on how to use them. More specifically, in South Africa, it was reported Dlamini & Ndzinisa, (2020b) that the students started studying online without enough preparation and that their access to digital learning materials was limited, preventing them from attaining the learning objectives. The main point here is that there was no prior training offered to university students when they transitioned from face-to-face training to online learning. Thus, the attention of the universities and the South African government was on the provision of digital technologies to students and university staff. Still, at the same time, less attention was given to the cyber safety of the end users. This would mean that the students would move into unfamiliar cyberspaces, increasing their vulnerability to cyber threats. The anticipated change in behaviour can be made through training to ensure that the students improve their understanding of cyber safety and threats.

The study's results advocated for training awareness campaigns on cybersecurity issues. According to Ajzen's (1991) theory of planned behaviour, a person's behaviour depends on their intention to carry out the behaviour. Additionally, subjective standards based on normative beliefs and a person's perceived behavioural control, which is reliant on control beliefs, all impact behaviour intention. This behavioural theory contends that it may be critical to disseminate knowledge to alter attitudes toward the desired behaviour (Lobe et al. 2011). The results of the study are in line with the findings by Zahidah et al., (2020), who did a study in Malaysia and stated that students need to be taught how to be safe and also how to govern the internet while at the same time not revealing a lot of personal information. The

findings are also corroborated by Alqahtani, (2022b), who claimed that one method is to raise risk awareness through educational materials and behaviour-related information. In the end, the significance of education and awareness-raising initiatives is to encourage student behaviour change, which indirectly lowers risky online behaviour.

The study results also indicated that some students had less knowledge of online risks. These findings are supported by Mpungose, (2020b), who indicated that some of the students lacked digital literacy, which is one of the needed skills to navigate the universities' digital technologies. More so, the study indicated that gaming could be used to draw students toward the risks associated with online learning and social media networks. The results are thus supported by Ticket al. (2021), who suggested that games can be used to increase digital literacy. Although students' grasp of the digital world has improved with time and exposure, it is far from assured that this awareness will translate into caution when safeguarding personal information. There is no one size fits for the measures that can be used to deal with students' daily learning cyber-crimes. Generally, the idea is to keep the students aware of the risks they face in online learning.

The study results indicated that students need to practice safe computing to minimise the effects of online risks, which they do not know. The same conclusions were made by Gabra et al., (2020a), who claimed that the best way to safeguard today's youngsters is to filter and prohibit unlawful and immoral websites. Setting up rules for Internet use at home, being responsible with how much time is spent online, choosing the right place for the computer, and keeping an eye on the information downloaded might help reduce these hazards.

The study found that students needed the topic of cyber safety to be covered in their curriculum, and Livingstone et al. (2017) found the same thing in a study conducted in the UK. They determined that the ability of people to apply skills, knowledge, and understanding to fully take advantage of the opportunities presented by the new media environment and protect themselves from related hazards may be referred to as "digital literacy." Although students' awareness of the digital world improves with time and experience, it is far from certain that this understanding leads to prudent behaviour concerning the security of personal data.

6.8 Summary

The chapter presented and discussed the study's results based on the primary data collected using online questionnaires. The results were presented following the research objectives formulated in Chapter 1. The initial hypotheses were tested for each objective, and conclusions were drawn. Literature from the second chapter was used to discuss the points of disagreement and points of agreement based on the already published results and what this study found out. The study's findings discussed applying the theory of planned behaviour, especially in influencing students to engage in risky online behaviours. The study found no one-size-fits-all solution for the measures that can be used to deal with the online risks students face in their day-to-day learning. Generally, the idea is to keep the students aware of the risks they face in online learning.

The chapter identified the chapter provided the students' views on their state of knowledge towards different forms of cyber threats and their attitude toward cyber safety. From their views, the researcher identified the measures needed to make the students cyber-safe and incorporated them into the cyber safety framework proposed for the study.

Based on the findings of this chapter, the next chapter looks at the contributions made by the current study compared with the previously written literature. The construction of a cyber security framework for first-year university students, which has been the major purpose of this study, will thus be discussed in the next chapter's essential success elements. The key success elements were determined based on expert assessments, internet survey results, and academic research. In the following chapter, the final framework will be discussed.

CHAPTER 7

CYBER SAFETY AWARENESS FRAMEWORK FOR FIRST-YEAR UNIVERSITY STUDENTS

7.1 Introduction

The previous chapter presented, analysed, interpreted, and discussed the research findings based on the data collected using online questionnaires. The findings were also discussed with the existing literature, and points of agreement and disagreement were noted and discussed. The chapter provided conclusions on the research hypotheses formulated in Chapter 1. The findings of the previous chapter are the key ingredients for developing the critical success factors and the final framework proposed in this study.

The challenge the study intended to solve was the lack of a framework for cyber safety awareness for first-year university students in developing countries, focusing on South Africa. The previous chapters (Chapter 2) looked at the theoretical underpinnings related to cyber security awareness based on the theory of planned behaviour. Chapter 3 looked at "cyber safety knowledge" and "cyber safety awareness." The chapter looked at the effect of cyber safety knowledge and attitude on cyber safety awareness. Chapter 4 covered the measures that need to be developed to establish the cyber safety framework. The methodology chapter (Chapter 5) looked at the philosophical perspective that influenced the study. Based on the study's findings, the students showed a lack of cyber safety knowledge and attitude toward cyber safety awareness.

This chapter, there is an identification of the critical success factors which are needed for the development of a cyber safety framework for university students. The factors are identified from the literature used in the study and the research findings based on data collected from the students using online questionnaires. More so, the initial models and the proposed frameworks are given to experts (lecturers in computer science and information systems) for their feedback. After three iterations (see Fig 7.2), the final cyber safety framework was formulated.

7.2 Framework for cyber safety awareness

The foundation for promoting cyber safety awareness is described in this subsection. The development of the framework went through three iterations which started from chapter 1 through the formulation of the research objectives which led to the researcher developing the research hypothesis (Figure 7.1). The elements of the objectives were then represented in the form of a conceptual framework which showed the relationship between the independent and the dependent variables. The literature evaluated in chapters 2, 3, and 4 served as the first entry point in this instance for the identification of critical success factors. The critical success factors were given to the experts for review. The critical success factors required for the student's understanding of cyber safety were produced as a result of the framework being provided to experts for assessment after it had been created (Figure 7.1). Furthermore, the study's findings and the literature were used to identify the critical success factors. A first proposed framework was created by reviewing the literature after the important success elements were returned to the experts for approval and this was presented in Figure 4.3. To create the study's final framework, the suggested cyber safety framework was once more distributed to experts for assessment. After the review from the experts the researcher developed a framework based on the findings from the online questionnaires from the students. The survey-based framework was also based on the hypotheses which the researcher formulated in Chapter 1. The survey-based framework was also given to the experts for review and based on the input from the experts, the proposed framework was produced (Figure 7.1).

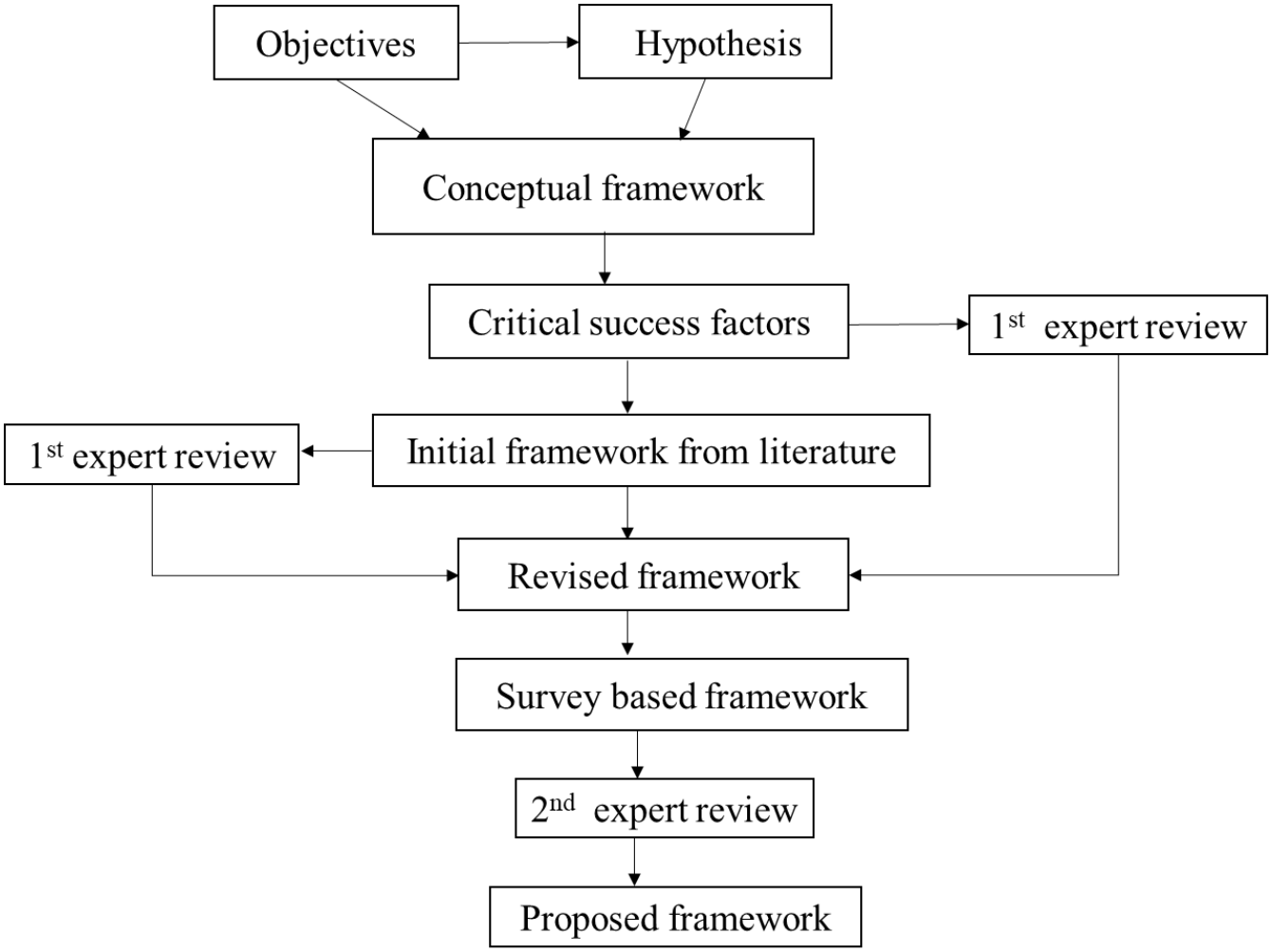


Figure 7.1: Iterative stages followed during the development of cyber safety awareness framework.

7.3 Survey based cyber-safety awareness framework

The 1st framework was based on extensive literature as presented in chapter 2, 3 and 4. Cyber safety awareness also included measures to minimize the risks associated with fraud, privacy breaches, malware, phishing, and scams. Thus, the model was developed through the integration of data collected from questionnaires. The survey based developed was shown in Figure 7.2.

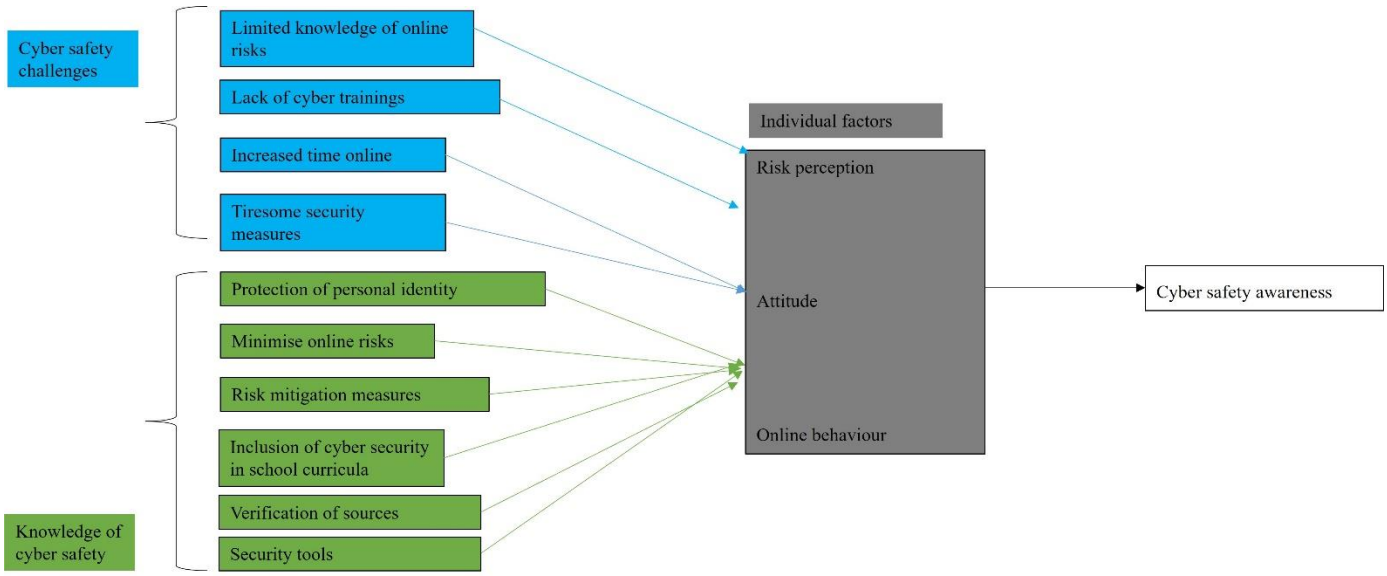


Figure 7.2: Survey based cyber-safety awareness framework

Figure 7.2 presented different cyber safety challenges faced by the students when having online access. The model categorized the factors into three major elements namely cyber safety challenges faced by the university students, their own cybersafety knowledge of the concept of cyber safety and individual factors which also affect their extent of being cyber aware. All the three factors when combined affected the level of cyber safety awareness of the university students. Some of the factors include knowledge of cyber safety, including individual factors such as online behaviour, attitude towards cyber safety and perception of risk. Under the cyber safety factor, it has been found out that students need to protect themselves from having their personal identity stolen and at the same time they need to know about the amount of time that they spend online. However, the increased online presence is not a deliberate move by the students but it is because of the Covid-19 pandemic which made changes between physical classes, wholly online and blended learning. All these shifts in the modes of learning meant that the students were spending more of their time online which was met with a lot of cyber threats. The results of the study even indicated that the more the students stay online the higher the risk of the students facing online risk. Since there are some students who indicated that they had less knowledge on some particular kinds of risks, they need to have knowledge about how to minimize the risks that they face when online. At the same time, the knowledge of risks and how to reduce them can be done when knowledge is imparted to the students and this can be done through the inclusion of cyber safety components in the university curricula especially for first year students. The students also

need to have knowledge of the security tools which they need to have in order for them to minimize the risk of online threats.

Under cyber safety challenges, the challenges which the students faced and these included the lack of knowledge on the online risks that they face and some of the challenges stem from the lack of educational foundation or training in cyber safety. The results presented in chapter 6 indicated that there are some students who did not know some cyber aspects such as phishing, sexting and identity theft. This meant that they cannot be aware of things that they had limited or no knowledge of. With the human being as the human link of cyber threat attacks, then lack of knowledge even made the university students without knowledge of the different risks more vulnerable. This study found out that the challenges the students face when online were due to their increased online presence and more precisely being online every hour. This meant that the more the students are online the more they are exposed to the online threats of different forms. The Covid-19 pandemic has exacerbated the frequency of student online as there has been a shift of the students from physical learning to wholly online and the use of blended learning. This meant that the students needed to be frequently online to meet up with the demands of their education but at the same time making them exposed to online threats of different forms. Moreso some of the students do not want to go through the security measures.

There are individual based factors which affect the ways in which the students engage on online usage. These include their perception of risk and attitude towards the measures which are used to reduce their online risk. Thus, there is need to make sure that there is minimization in the weakest link of the human being and in the case of this study the students through a number of ways such as training and awareness campaigns. However in the in the context of South Africa, the students began learning online without proper preparation and their access to digital learning resources is minimal affecting them from achieving the learning goals. It is the lack of training which made the students more vulnerable to online risks during the learning time under the Covid-19 pandemic. In this case as there are some students who had a different attitude towards cyber safety, their likelihood of doing the same risky behaviour was high. In some case it can be assumed that the level of knowledge about online risk would develop cautious behaviour regarding personal data protection although there is uneven digital literacy. The need to look at the safety of the students emanate from

the view that there are changes in attitude, behaviour and perception which are brought about by the changes in technology.

7.3.1 Review of the survey-based framework by experts

The survey-based framework was also given to the identified experts who were used to review the critical success factors and the initial model developed from literature. The major feedback from the experts was that the survey-based model did not cover the other elements which were covered in the conceptual models which was in line with the objectives and the hypotheses formulated in Chapter 1. The reviewers recommended that I include the method which I would use to be able to deal with the factors needed raised the survey using the online questionnaires. The NIST cybersecurity framework was once again suggested to be included in the revised model especially from a methods perspective especially training and awareness, governance and policies towards cyber security. The feedback of the model indicated that there are some missing elements in the model especially on the challenges which affect the students when online and their viewpoints were thus required by the experts. Thus, the researcher looked at the framework and took out elements which were related to the students or the human element. Thus, the next subsection proposed cyber safety awareness among university students.

7.4 A framework for cyber safety awareness amongst first year university

Information from the experts used in the proposed framework for cyber safety awareness is presented in Figure 7.3. The proposed framework comprises three main components that can be used to ensure the safety of the students: knowledge capacitation, risk/time awareness, and an attitude towards cyber safety measures and increased cyber safety awareness. In this case, knowledge capacitation involves informing the students about threats such as phishing, sexting, and identity theft. There are protective measures that are needed to be taken by the students, and these include the installation of firewalls and anti-malware software. However, to be able to achieve the knowledge capacitation, there is a need to have cyber safety issues included in the university curriculum, especially for the first years. The use of education can be combined with implementing the South African National Cybersecurity Policy Framework

(NCPF), whose thrust is cyber security education. According to the NCPF, there is a need to create an enabling environment for cybersecurity education and guide the implementation and development of an environment that fosters cybersecurity education (Waldock et al., 2022). Thus, it is the university's responsibility to comply with the demands of an NCPF. Moreso, there is a need to combine awareness, attitude, and knowledge to promote secure online behaviour among university students. Therefore, the factors used in developing the framework cannot be used in isolation for improved cyber safety awareness; they need to be combined. The use of workshops will capacitate the human mind about the protective measures used to reduce online risks. Human factors define how one perceives risk, which leads to the types of online behaviour in which one engages on the internet (NIST, 2018). This entails the types of websites visited and the time spent online. All these factors ensure the vulnerability of the users as they use the internet.

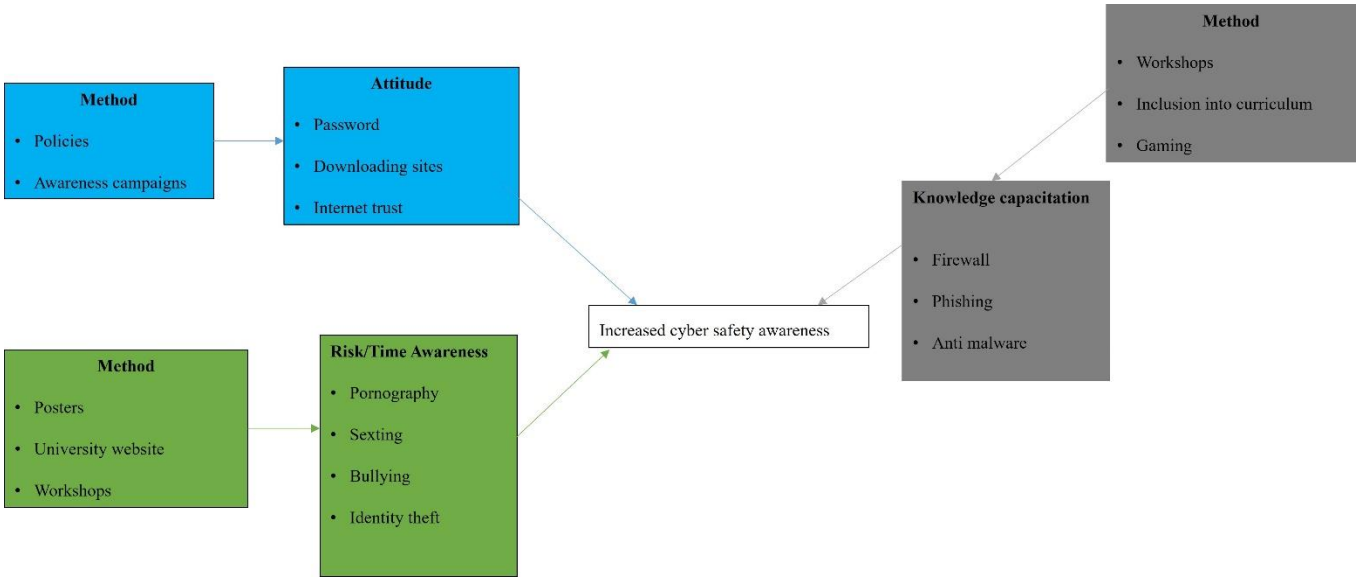


Figure 7.3: Proposed cyber safety framework for the study

The other aspect is risk/time awareness, in which the university is informed about the time they spend online and the associated risks they face. These awareness functions can be done through posters and university websites, informing the students of the dangers that they face online. Posters can be pasted on the university walls of cafeterias to grab the students' attention in places where they usually meet up (Marinoni et al., 2020). This has been regarded as an effective strategy as it can emphasise time-sensitive issues to individuals. Posters can be used to inform individuals about their safety when online. In this case, the university can share with students examples of phishing emails and fake job alerts that can steal their

identity. This makes them more aware of the risks they likely face online. The awareness campaign will be done to inform university students that pornographic sites, sexting, bullying, and identity theft are some of the online threats that they face. It is expected that through the awareness campaigns, the knowledge generated through games and training can be used to affect human factors such as perception of risk and online behaviour and develop the students' safe computing skills. Through the training, students gather knowledge on the different types of online attacks, reducing their vulnerability. Games are incorporated into the learning curricula as a model that can simulate cyber-safety activities in a way that attracts students. The main aim of games is to increase awareness about cyber safety, which in a way, can lead to certain online behaviour among university students (Shakeel et al., 2022). Through training, it is anticipated that verification of sources of information, no matter how authentic they look, maybe another way to reduce internet risks. This will also lead to an increase in how one can protect themselves, making it safer to use the internet.

The training also debunks the misconception that the installation of anti-virus is enough to protect their electronic gadgets and that firewalls are synonymous with anti-virus Mishna et al., (2010). Increasing cyber security awareness through training programs that expose students to cyber security defence tools through theoretical lectures and simulations. These would emphasise the operational, use, and procedural elements of enhancing user comprehension and turning it into efficient cyber security mitigation behaviour. Gaming could draw students toward the risks associated with online learning and social media networks. Ticket al. (2021) suggested that games can be used to increase digital literacy. Although students' grasp of the digital world has improved with time and exposure, it is far from assured that this awareness will translate into caution when safeguarding personal information. There is no one size fits all for the measures that can be used to deal with students' daily learning cyber-crimes.

The other element of the cyber safety framework is the attitude toward cyber safety measures, including password-strengths issues. However, there is a misconception that one will be protecting oneself with a unique password, and there is no need to worry about other cyber security threats (Hunt, 2016). Creating unique passwords is a commendable positive start. Still, it is insufficient to prevent hackers from accessing user information owing to their knowledge of and access to technology that may decode passwords or perform a password bypass (Hunt, 2016). The university needs to develop a system that prompts students to

generate passwords that are not their names or dates of birth, use alphanumeric characters, and have a certain number of characters. At the same time, the university can also make sure that the university students change their passwords once every six months and do not repeat an old password. These elements in the framework need not be used in isolation, as the students can develop a false sense of security, leaving them vulnerable to other online risks. The students also need to have a positive attitude toward the sites they can visit and understand that there is a digital footprint on the sites that they visit. In as much as there is the use of passwords and firewalls, the students, through awareness campaigns, will be taught about the dangers of online trust as this can lead to identity theft. Therefore, university policies about the sites to be visited by the students and awareness campaigns can make the students change their attitude towards cyber safety awareness.

7.5 Summary

Through the reviews by the experts, the researcher managed to identify the critical success factors needed for developing the cyber safety framework. In the chapter, the researcher developed a cyber safety framework for Eastern Cape, South Africa, university students.

The study aimed to develop a cyber safety framework for university students. As such, there was a need to identify the critical success factors the students would need to develop cyber safety. The developed framework was the product of three elements. The researcher and the reviewers developed the initial framework, and the feedback from the students came through questionnaires. Literature was used to develop some critical success factors, and support from the various authors was shown. Based on the expert reviews, a student-centred framework was suggested, which meant an intersection between literature and research findings was suggested. The experts suggested an overlap between literature and research findings, and the factors that overlapped were used to develop the proposed framework. Through the use of expert reviews, the initial model and critical success factors were modified and refined.

The next chapter provides a conclusion and summary of this research. The next chapter summarises the research objectives, an evaluation of the research, and the study's contribution. In the chapter, there is coverage of the study's limitations and directions for further research.

CHAPTER 8

CONCLUSION

8.1 Introduction

The previous chapter presented the critical success factors and the proposed cyber safety framework model for Eastern Cape, South Africa, university students. The frameworks were developed after reviewing them by computer science and information systems experts.

The first chapter sets out the context of the study by showing the research gaps that the study intended to fill in the context of cyber safety awareness among first-year university students in the Eastern Cape, South Africa. In the first chapter, the hypotheses were laid out and tested when the results were presented and discussed. The theoretical framework guiding the study presented in Chapters 2, 3, and 4 provided the discussion points in Chapter 6 when the results were discussed. Chapter 5 on research methodology discussed the research philosophy which influenced the research design and data analysis methods.

The previous chapters aimed to provide a framework for cyber safety awareness among first-year university students in the Eastern Cape. Different steps, such as expert reviews, results from questionnaires, and literature review, led to modifications and development of the proposed framework. This sub-section of the study provides the conclusions of the study based on the research findings presented in chapter 6. Based on the study's shortcomings, some recommendations will be formulated to make areas that need further research.

8.2 Recap of the research objectives

The primary research goal of this study was to provide a framework for first-year students in the Eastern Cape, South Africa, to be aware of cyber safety. It had a variety of goals to achieve this. Chapter 7 of the research contains the proposal for the framework. Four sub-research objectives were developed for the study, nevertheless, to address the main research topic.

1. *To identify the online risks facing first-year students at a selected university in Eastern Cape*

The research findings of the study, based on data collected using online questionnaires, indicated that the leading online risks faced by university students were cyberbullying, phishing scams, identity fraud, invitations to pornography, and sexting. Some of the online risks identified in the study are in line with most of the published literature on the subject matter. Differences in the findings of the study and those published in the literature indicate the differences in the social, economic, and cultural contexts in which the studies were carried out.

2. *To determine the effect of cyber security knowledge on cyber safety awareness among first year students in Eastern Cape*

Results of the study indicated that most students were knowledgeable about the different aspects of cyber security issues. However, some students showed that they did not know about some cyber security aspects, such as making use of firewalls and phishing. It is from the lack of knowledge that the research intended to develop a framework to make sure that these are catered for to reduce their online risk and make them cyber secure. The literature also noted that the levels of knowledge about cyber issues are country-specific; some students have basic knowledge, yet those with advanced knowledge can still be reckless about their digital footprint on the internet.

3. *To examine the effect of cyber security attitude on cyber safety awareness of first year students in Eastern Cape*

Based on student responses to questionnaires, it was deduced that the students had a negative attitude towards strong passwords and used common passwords such as names. Students had mixed attitudes towards cyber safety awareness, such as posting pictures, security, and updating software, which is time-consuming. From the literature, it was noted that, based on the Theory of Planned Behavior, attitude is central to behaviour control. Some of the elements discussed here led to the development of the initial and final models about cyber safety awareness among

4. *To develop measures for addressing cyber safety awareness challenges among first year students in Eastern Cape*

Measures that were stated to deal with the challenges faced by students were providing training and awareness campaigns, changing passwords frequently, and having cyber safety aspects included in their curriculum. The literature also stated through the Theory of Planned

Behaviour that behaviour is a function of the intentions to do a specific behaviour. In the literature, it was noted that digital literacy, including cyber safety, could be increased through participation in games.

Table 8.1: Summary of the objectives, research questions and conclusions for the study

Objectives	Research question	Research design	Results	Conclusions
Main objective: To develop a framework for cyber safety awareness amongst first year students in the Eastern Cape, South Africa.	**Main research question:** How can cyber safety awareness challenges be addressed among first year students in the Eastern Cape?	Mixed methods	A cyber safety awareness framework for first year student was developed	Student's attitude, risk time awareness and knowledge capacitation are the factors needed to develop the cyber safety awareness framework
Objective 1: To identify the online risks facing first-year students at a selected university in Eastern Cape	**Research question 1**: Which online risks are faced by first-year students in the Eastern Cape?	**Method 1**: Descriptive	**Result 1**: Main online risks that university students faced were cyberbullying, phishing scams, identity fraud, invitations to pornography and sexting. Time spent online is significantly associated with the likelihood of facing online risks	Conclusion 1: The students are faced with several online risks. The more time the students spend online, the more online risks they face.
Objective 2: To determine the effect of cyber security knowledge on cyber safety awareness among first year students in Eastern Cape	**Research question 2**: How does cyber security knowledge affect cyber safety awareness among first year students in the Eastern Cape?	**Method 2**: Descriptive	**Result 2**: Mixed results, with some students knowledgeable and others not having cyber knowledge about the different online threats. A statistically	**Conclusion 2.** The level of cyber security knowledge leads to cyber safety awareness among first year students in Eastern Cape

			significant association between cyber security knowledge and cyber safety awareness among first year students in Eastern Cape	
Objective 3: To investigate the impact of cyber security attitudes on first-year students' understanding of cyber safety in the Eastern Cape	**Research question 3**: What is the cyber security attitude's effect on first-year students' cyber safety awareness in the Eastern Cape?	**Method 3**: Descriptive	**Result 3:** Mixed cyber security attitudes affect the level of cyber safety awareness. A statistically significant association between the student's attitude and cyber safety awareness.	**Conclusion 3:** Positive cyber security attitude leads to cyber safety awareness.
Objective 4: To develop measures for addressing cyber safety awareness challenges among first year students in Eastern Cape	**Research question 4**: What measures can be developed to address cyber safety awareness challenges among first year students in Eastern Cape?	**Method 4**: Qualitative	**Result 4:** Critical success factors are needed to develop a cyber safety framework. The factors required for the development of the framework include attitude, risk time awareness and knowledge capacitation	**Conclusion 4**: The factors required for the development of the framework include attitude, risk time awareness and knowledge capacitation

8.3 Theoretical framework

The study reviewed theories of human behaviour and how they relate to understanding cyber safety in chapters 1 and 2. It was simple to discuss the research results and create a framework for cyber safety awareness among university students, thanks to a literature

review. The literature was also examined to identify the important success criteria that may be used to raise students' understanding of online safety issues. The Theory of Planned Behaviour (TPB), proposed by Ajzen (1991) as an expansion of the Theory of Reasoned Action, was one of the three theories discussed in this study. The TPB aims to offer a framework for predicting actual behaviour and behavioural intentions. Attitude, perceived standards, and perceived behaviour control all influence one's propensity to engage in certain behaviours. The TPB was expanded to include other variables, including knowledge and individual experiences, as these variables directly affected a person's attitude. The user's attitude might be affected by their understanding of cyber safety. One factor influencing attitude is awareness of hazards in the context of information, communication, and technology (ICT) (Vafaei-Zadeh et al., 2019).

The study also looked at the Social Learning Theory (SLT) that was put forward by (Akers, 1985, 1998), basing it on the behavioural learning approach. In theory, there is a utilization of the learnt behaviour and differential association (Bada et al., 2019). Thus, differential association is related to how people interact and how the associations with different people impact their values and norms (Bhatnagar & Pry, 2020). The first group of people that affect family and friends' behaviour and the associations that happen at an early stage in life tend to last longer, affecting the individual's behaviour. This concept relates to the proposed study because the first-year students' associations affect the individual's online behaviour and the associated challenges. The other concept of the SLT is an attitude, which implies how a person perceives good and bad (Gabra et al., 2020a). Specifically, the study refers to how an individual views online behaviour and cyber safety awareness among first-year students at selected universities in the Eastern Cape.

The third theory used in the study was the NIST cyber security framework and ISO/IEC 27001 standard (NIST, 2018). The NIST framework suggests several factors that can be used to develop a cyber security framework. The human-centred ones include human factors, the role played by awareness and campaigns, governance, policy, and technical skills. Therefore, the NIST framework is a source of critical success factors for developing the cyber safety framework. Thus, from the three theories, there was a discussion of the research findings, identifying the critical success factors and the cyber safety framework.

8.4 Research methodology

This study was guided by the pragmatism research paradigm, which detached the researcher from the participants, making the collection of data independent. The research paradigm meant that the study was quantitative, and online questionnaires were used to collect data from university students. The online questionnaires used a Likert scale that ranged from 1 to 4, which meant: "Strongly Agree" = 1, "Agree" = 2, "Disagree" = 3, and "Strongly Disagree" = 4. In the questionnaire where the questions had a negative implication they were reverse coded implying that "Strongly disagree" =1, "Disagree" =2, "Agree" =3, and "Strongly agree" =4. The Likert scale meant that the researcher could calculate descriptive statistics such as mean and standard deviation to determine the general perception of the university students. The research also used expert knowledge to get feedback on the initial model, critical success factors, and the final cyber safety framework.

8.5 Evaluation of the research

The evaluation of the research meant that the research was viewed as trustworthy and credible, in line with the Oates (2006) research criteria for pragmatism-inclined research. The elements specific to this research, since it was pragmatic, included the following:

1. *Validity* was determined for the framework, which was given to experts in information systems and computers for their review. Since these are experts in the field, their feedback on the framework was regarded as valid.

2. *Objectivity* was gained with the pragmatism paradigm, which meant that the research was objective and independent as the research was not influential in the data collection process as data was collected online. The use of experts meant they gave an objective evaluation of the cyber safety framework based on theoretical underpinnings.

3. *Reliability* was tested using Cronbach's alpha test in which the scale items of knowledge, attitude, measures, and effects of knowledge on cyber safety were tested. Overall all the factors were deemed reliable (apha=0.772). The expert reviews were regarded as reliable as they knew the field.

4. *Internal validity* was achieved through many data collection and analysis methods.

5. *External validity* can be noted through the developed cyber safety framework, which can be extended to other students or people under the same circumstances.

Having looked at all the criteria above based on Oates (2006), it can be stated that the researcher believed the study was credible.

8.6 Contribution of the study

Less attention has been paid to providing a cyber safety framework across large and diverse populations in South Africa, especially among university students (Walaza et al., 2014, Catota et al., 2019). Based on the background above, the study intended to develop a cyber safety framework for university students. Thus, the research contributes knowledge through the framework to increase cyber safety among university students. The framework also mainly provided a student-centred framework that pinpointed their human behaviour, knowledge, and technological skills, changing their cyber safety attitudes.

8.7 Limitations of the study

The study dealt with university students' cyber safety based on their online risks, their knowledge about the threats they faced online, and the attitude and measures they used. However, the limitation of the study was not to determine the knowledge and attitude toward cyber safety across a socio-economic gradient. This will have meant that the challenges or the measures will be developed targeting a particular section of society. The other limitation of the study was that it did not focus on the institutions to determine their viewpoints on the kind of cyber safety measures that they offer to their students.

8.8 Directions for further research

Since the study showed that more females took part in the study and the dominant age group was 18–24years, further research can be age and gender specific to determine the effectiveness of measures to ensure cyber safety. In the future, trend analysis can be determined with the introduction of different measures of cyber safety to measure their effectiveness. Further research can use the proposed framework and test its effectiveness on the knowledge and measures about cyber safety.

8.9 Summary

The chapter provided a summary of the fundamental research by summarising the research objectives, theoretical frameworks, and the research methodology used in the study. The chapter also looked at the Oates (2006) research criteria for pragmatism-inclined research and

how the research met the demands. The chapter examined the theoretical framework and how it affected the final model's development and identified the crucial success factors. The conclusion examined the research paradigm, the Oates (2006) research standards, and Hevner, March, Park, and Ram's (2004) recommendations.

The lack of a cyber safety awareness framework in South Africa, particularly among university students, has given rise to the framework that has been presented. In this instance, the study's product was a suggested framework for online safety for university students in the Eastern Cape, aiming to decrease risk, particularly due to rising levels of blended learning during the COVID-19 epidemic. The chapter also considered the study's contribution, the suggested framework for cyber safety, and potential future research fields.

REFERENCES

Ajzen, I. (1991). The theory of planned behaviour. *Organisational Behaviour and Human Decision Processes*, *50*(2), 179–211.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 1–15. https://doi.org/10.3390/bdcc5020023

Alhejaili, H. (2013). *Usefulness of teaching security awareness for middle school students* [MSc thesis]. Rochester Institute of Technology.

Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and Information Technologies*, *25*(6), 5261–5280. https://doi.org/10.1007/s10639-020-10219-y

Alotaibi, N. B., & Mukred, M. (2022). Factors affecting the cyber violence behavior among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA. *Technology in Society*, *68*, 101863. https://doi.org/10.1016/j.techsoc.2022.101863

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, *12*(5), 1–21. https://doi.org/10.3390/app12052589

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(e06016), 1–13. https://doi.org/10.1016/j.heliyon.2021.e06016

Asanan, Z. Z. T., Hussain, I. A., & Laidey, N. M. (2017). A Study on Cyberbullying: Its Forms , Awareness and Moral Reasoning Among Youth. *International Journal of Information and Communication Sciences*, *2*(5), 54–58. https://doi.org/10.11648/j.ijics.20170205.11

Bada, M., & Sasse, A. (2014). *Cyber Security Awareness Campaigns Why do they fail to change behaviour?* Global Cyber Security Capacity Centre.

Bada, M., von Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness for Users and Executives in Africa. *International Journal on Advances in Security*, *12*(1), 108–118.

Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational Research: Determining Appropriate Sample Size in Survey Research. *Information Technology, Learning, and Performance Journal*, *19*(1), 43–50.

Bhatnagar, N., & Pry, M. (2020). Student attitudes , awareness , and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal*, *18*(1), 48–58.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. University of South Florida.

Burns, S., & Roberts, L. (2013). Applying the Theory of Planned Behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48–64. https://doi.org/10.1057/cpcs.2012.13

Chandarman, R., & van Niekerk, B. (2017). Students ' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication*, *20*, 133–155. https://doi.org/10.23962/10539/23572

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

Choejey, P., Murray, D., & Che Fung, C. (2016). Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations. *Computer Science & Information Technology (CS & IT)*, 49–61. https://doi.org/10.5121/csit.2016.61505

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (4th ed). Pearson.

Custodio, E. B., & Malawit, G. M. (2020). Cybersecurity for higher education institutions: Adopting regulatory framework. *Global Journal of Engineering and Technology Advances*, *2*(3), 016–021. https://doi.org/10.30574/gjeta.2020.2.3.0013

de Barros, M. J. Z., & Lazarek, H. (2018). A Cyber Safety Model for Schools in Mozambique. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, *Icissp*, 251–258. https://doi.org/10.5220/0006573802510258

Dlamini, R., & Ndzinisa, N. (2020). Universities trailing behind: Unquestioned epistemological foundations constraining the transition to online instructional delivery and learning. *South African Journal of Higher Education*, *34*(6). https://doi.org/10.20853/34-6-4073

Floress, K., Huff, E. S., Snyder, S. A., Koshollek, A., Butler, S., & Allred, S. B. (2019). Factors associated with family forest owner actions: A vote-count meta-analysis. *Landscape and Urban Planning*, *188*, 19–29. https://doi.org/10.1016/j.landurbplan.2018.08.024

Gabra, A. A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber Security Awareness Among University Students: A Case Study. *International Journal of Advance Science and Technology*, *29*(10), 767–776.

Garba, A., Sirat, M. B., Siti, H., & Dauda, I. B. (2020). Cyber Security Awareness Among University Students: A Case Study. *International Journal of Advance Science and Technology*, *2*(1), 82–86. https://doi.org/10.31580/sps.v2i1.1320

Giannakas, F., Kambourakis, G., Papasalouros, A., & Gritzalis, S. (2016). Security Education and Awareness for K-6 Going Mobile. *International Journal of Interactive Mobile Technologies*, *10*(2), 41. https://doi.org/10.3991/ijim.v10i2.5473

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Gumede, L., & Badriparsa, N. (2022). Online teaching and learning through the students' eyes – Uncertainty through the COVID-19 lockdown: A qualitative case study in Gauteng province, South Africa. *Radiography*, *28*(1), 193–198. https://doi.org/10.1016/j.radi.2021.10.018

Gundu, T., Maronga, M. I., & Boucher, D. (2019). Industry 4.0 Business Perspective: Fostering a Cyber Security Culture in a Culturally Diverse Workplace. *Kalpa Publications in Computing*, *12*, 85–94.

Harris, L., & Brown, G. (2010). Mixing interview and questionnaire methods: Practical problems in aligning data. *Practical Assessment, Research and Evaluation*, *15*(1).

Hedding, D. W., Greve, M., Breetzke, G. D., Nel, W., & Jansen van Vuuren, B. (2020). COVID-19 and the academe in South Africa: Not business as usual. *South African Journal of Science*, *116*(7/8). https://doi.org/10.17159/sajs.2020/8298

Hunt, T. (2016). *Cyber Security Awareness in Higher Education*. Central Washington University.

Kovacevic, A., & Radenkovic, S. D. (2020). SAWIT — Security Awareness Improvement Tool in the Workplace. *Applied Sciences*, *10*(103065), 1–13.

Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal*, *29*(2), 16–35.

Kritzinger, E., Bada, M., & Nurse, J. R. C. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. *10th World Conference on Information Security Education (WISE)*, 1–10.

Kritzinger, E., Loock, M., & Goosen, L. (2019). Cyber Safety Awareness – Through the Lens of 21st Century Learning Skills and Game-Based Learning. *Innovative Technologies and Learning: Second International Conference, ICITL 2019, Tromsø, Norway, December 2–5, 2019, Proceedings*, *11937*. https://doi.org/10.1007/978-3-030-35343-8

Laher, S., Bain, K., Bemath, N., de Andrade, V., & Hassem, T. (2021). Undergraduate psychology student experiences during COVID-19: Challenges encountered and lessons learnt. *South African Journal of Psychology*, *51*(2), 215–228. https://doi.org/10.1177/0081246321995095

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Le Grange, L. (2021). Covid-19 pandemic and the prospects of education in South Africa. *PROSPECTS*, *51*(1–3), 425–436. https://doi.org/10.1007/s11125-020-09514-w

Marinoni, G., van't Land, H., & Jensen, J. (2020). *The impact of Covid-19 on higher education around the world* (p. 50). International Association of Universities.

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2020). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security Privacy*, 1–11. https://doi.org/10.1002/spy2.141

Mishna, F., Cook, C., Gadalla, J., Daciuk, J., & Solomon, S. (2010). Cyber Bullying Behaviours among Middle and High School Students. *American Journal of Orthopsychiatry*, *80*(3), 362–374. https://doi.org/10.1111/j.1939-0025.2010.01040.x

Mncedisi, C. M., Nontobeko, P. K., & Khumalo, P. N. (2021). Student teachers' experiences of the emergency transition to online learning during the COVID-19 lockdown at a South African university. *Perspectives in Education*, *39*(3). https://doi.org/10.18820/2519593X/pie.v39.i3.4

Mpungose, C. B. (2020). Emergent transition from face-to-face to online learning in a South African University in the context of the Coronavirus pandemic. *Humanities and Social Sciences Communications*, *7*(1), 1–9. https://doi.org/10.1057/s41599-020-00603-x

Muhirwe, J., & White, N. (2016). Cybersecurity awareness and practice of the next generation corporate technology users. *Issues in Information Systems*, *17*(II), 183–192. https://doi.org/10.48009/2_iis_2016_183-192

Mukuna, K. R., & Aloka, P. J. P. O. (2020). Exploring Educators' Challenges of Online Learning in Covid-19 at a Rural School, South Africa. *International Journal of Learning, Teaching and Educational Research*, *19*(10), 134–149. https://doi.org/10.26803/ijlter.19.10.8

Ntombela, S. (2022). Reimagining South African higher education in response to Covid-19 and ongoing exclusion of students with disabilities. *Disability & Society*, *37*(3), 534–539. https://doi.org/10.1080/09687599.2021.2004880

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN EleSprouts: Working Papers on Information Systemsctronic Journal*, *10*(26), 1–46. https://doi.org/10.2139/ssrn.1954824

Olaniran, S. O., & Uleanya, C. (2021). The Effects of COVID-19 on International Students in South Africa. *International Journal of Innovation*, *15*(4), 13.

Pillay, A., Khosa, M., Sheik, A., Campbell, B., Mthembu, B., & Nyika, N. (2021). How Home Contexts of South African University Students Shape their Experiences of

Emergency Remote Teaching and Learning. *Student Success*, *12*(2). https://doi.org/10.5204/ssj.1779

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 1–25. https://doi.org/10.1016/j.ijcci.2021.100343

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). *Planning for cybersecurity in schools: The human factor*. *27*(2), 17.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Salami, J. (2021). *COVID's Lessons for Global Higher Education* (Vol. 0). Lumina Foundation. http://journals.sagepub.com/doi/10.1177/14782103211021937

Shakeel, T., Habib, S., Boulila, W., Koubaa, A., Javed, A. R., Rizwan, M., Gadekallu, T. R., & Sufiyan, M. (2022). A survey on COVID-19 impact in the healthcare domain: Worldwide market implementation, applications, security and privacy issues, challenges and future prospects. *Complex & Intelligent Systems*. https://doi.org/10.1007/s40747-022-00767-w

Siyam, N., & Hussain, M. (2021). Cyber-Safety Policy Elements in the Era of Online Learning: A Content Analysis of Policies in the UAE. *TechTrends*, *65*(4), 535–547. https://doi.org/10.1007/s11528-021-00595-8

Smit, D. M. (2015). Cyberbullying in South African and American schools: A legal comparative study. *South African Journal of Education*, *35*(2), 1–11. https://doi.org/10.15700/saje.v35n2a1076

Staksrud, E., & Livingstone, S. (2009). Children and online risk: Powerless victims or resourceful participants? *Information, Communication & Society*, *12*(3), 364–387. https://doi.org/10.1080/13691180802635455

Stockemer, D. (2019). *Quantitative Methods for the Social Sciences: A practical introduction with Examples in SPSS and Stata*. Springer International Publishing.

Thaba-Nkadimene, K. L. (2020). Editorial: COVID-19 and e-learning in higher education. *Journal of African Education*, *1*(2), 5–11. https://doi.org/10.31920/2633-2930/2020/1n2a0

Tick, A., Cranfield, D. J., Venter, I. M., Renaud, K. V., & Blignaut, R. J. (2021). Comparing Three Countries' Higher Education Students' Cyber Related Perceptions and Behaviours during COVID-19. *Electronics*, *10*(22), 2865. https://doi.org/10.3390/electronics10222865

Tsokota, T., Mhloza, V., & Chipfumbu-Kangara, C. (2022). A strategy to enhance e-safety among first-year students at Zimbabwean universities: An action research. *Educational Technology Research and Development*, *70*(2), 639–655. https://doi.org/10.1007/s11423-022-10078-z

Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes*, *48*(8), 1565–1585. https://doi.org/10.1108/K-05-2018-0226

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's." *Heliyon*, *5*(12), 1–8. https://doi.org/10.1016/j.heliyon.2019.e02855

Waldock, K. E., Miller, V., Li, S., & Franqueira, V. N. L. (2022). *Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people* (p. 159). InstituteofCyberSecurityforSociety(iCSS).

Wang, L., & Alexander, C. A. (2021). Cyber security during the COVID-19 pandemic. *AIMS Electronics and Electrical Engineering*, *5*(2), 146–157. https://doi.org/10.3934/electreng.2021008

Zulkifli, Z., Molok, N. N. A., Rahim, N. H. A., & Talib, S. (2020). Cyber security awareness among secondary school students in Malaysia. *Journal of Information Systems and Digital Technologies*, *2*(2), 28–41.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

APPENDICES

Appendix 1: Online questionnaire

My name is Everjoy. C. Makazhe doing a Master of Commerce in Information Systems with the University Y. I am carrying out a research entitled: **A framework for cyber safety awareness amongst first year students in the Eastern Cape, South Africa**. Confidentiality will be respected because the information gathered during this time will only be utilized for academic and research reasons. Please answer all of the questions on the following questionnaire honestly. You are free to decline research participation, and you can leave the study whenever you choose.

SECTION A: DEMOGRAPHIC BACKGROUND

1a. Age (if you are below the age of 18 don't proceed with the survey)

i. 18-20 ☐

ii. 21-25 ☐

iii. 26-30 ☐

1b) Gender

1. Male ☐ 2. Female☐

1c) Years using a computer or smartphone

i. 0-2 ☐

ii. 3-5 ☐

iv. 6-9 ☐

v. 10+ ☐

1.d) Online frequency

Online frequency	Tick
Always online	☐
Every hour	☐
Half a day	☐
Once a week	☐
After work	☐
Others specify…….	

SECTION B: Online risks are faced by first year students in Eastern Cape

Online risks	Tick
Sexting	☐
Cyber bullying	☐
Identify fraud	☐
Phishing scams	☐
Invitations to pornography	☐
Others specify…….	

SECTION C: Effects of cyber security knowledge on safety awareness among first year students in Eastern Cape

1. Knowledge on cyber security aspects

Knowledge on:	Very knowledgeable	Knowledgeable	I don't know
Phishing	☐	☐	☐
Usage of anti-virus software	☐	☐	☐
Making use of a firewall	☐	☐	☐
Identity theft	☐	☐	☐
Password security	☐	☐	☐
Cyber bullying	☐	☐	☐
Downloading and sharing pirated content	☐	☐	☐
Other specify……	☐	☐	☐

2. Effects of cyber security knowledge on safety awareness among first year students in Eastern Cape

View or Opinion	Strongly agree	Agree	Disagree	Strongly disagree
I am not ignorant of security concerns regarding smartphones	☐	☐	☐	☐
I am not fully aware of all the security risks and necessary security practices.	☐	☐	☐	☐
I never share my password or post it where others may obtain access to it	☐	☐	☐	☐
I know how to protect against 'social engineering' 'phishing' and 'cyber crime'	☐	☐	☐	☐
When away, I always lock my PC and employ my system's password protected screen saver	☐	☐	☐	☐
I am careful when opening email attachments and links	☐	☐	☐	☐
I do not use mobile applications which request for accessing your contacts, camera or location	☐	☐	☐	☐
Other specify……	☐	☐	☐	☐

SECTION D: Effect of cyber security attitude affect cyber safety awareness are faced by first year students in Eastern Cape

View or Opinion	Strongly agree	Agree	Disagree	Strongly disagree
It is a waste of time to change passwords because you can still get hacked	☐	☐	☐	☐
It is too difficult to remember difficult passwords; therefore I use my name or something easy to remember.	☐	☐	☐	☐
Posting pictures and bad messages online about my college students makes it anonymous and is much better than saying it to their face.	☐	☐	☐	☐
The security settings and tools slow me down and are pesky. I turn them off or disable them.	☐	☐	☐	☐
Updating my security software and Windows /Apple is too time consuming, annoying and uses up my bandwidth/ data bundle.	☐	☐	☐	☐
Other specify……	☐	☐	☐	☐

SECTION E: Solutions to cyber safety awareness challenges be addressed among first year students in Eastern Cape

View or Opinion	Strongly agree	Agree	Disagree	Strongly disagree
Training and awareness campaigns	☐	☐	☐	☐
Frequent secure password changes	☐	☐	☐	☐
Practising safe computing	☐	☐	☐	☐
Incorporate cyber security issues in the curriculum	☐	☐	☐	☐
Gaming for cyber security awareness	☐	☐	☐	☐
Development of cyber security policy or framework	☐	☐	☐	☐
Other specify……	☐	☐	☐	☐

THANK YOU FOR YOUR TIME

Appendix 2: Permission to carry out research

DIVISION OF ACADEMIC AFFAIRS AND RESEARCH
DIRECTORATE OF RESEARCH AND INNOVATION

01 September 2022

Everiov Chipo Makazhe

Department of Finance
MTHATHA
5100

Dear Ms Makazhe,

Gatekeepers Permission Letter to conduct research at Walter Sisulu University

Ethical Clearance Number: PID011SMAK01

Institution:

A Gatekeeper Letter is hereby granted for the study "**A framework for cyber safety awareness amongst first year students in the Eastern Cape, South Africa.**" provided that copies of your completed study will be submitted to the Campus Rector of the campus in which the study will be conducted and the Directorate of the Research & Innovation.

All data pertaining to Walter Sisulu University will be treated confidentially and you are required to abide by ethical principles at all times. It is your responsibility to seek consent from Participants.

Kind regards

Directorate: Research Development

Prof W Akpan
Senior Director: Research & Innovation

Appendix 3: Ethical clearance

ETHICS CLEARANCE
REC-270710-028-RA Level 01

Project Number:	PID011SMAK01
Project title:	**A framework for cyber safety awareness amongst first year students in the Eastern Cape, South Africa.**
Qualification:	Master of Commerce in Information Systems
Student name:	Everjoy Chipo Makazhe
Registration number	201820467
Supervisor:	Prof R Piderit
Department:	Information Systems
Co-supervisor:	Dr E Chindenga Mr M Mamba

On behalf of the University of Fort Hare's Research Ethics Committee (UREC) I hereby grant ethics approval for PID011SMAK01. This approval is valid for 12 months from the date of approval. Renewal of approval must be applied for BEFORE termination of this approval period. Renewal is subject to receipt of a satisfactory progress report. The approval covers the undertakings contained in the above-mentioned project and research instrument(s). The research may commence as from the 11/08/22, using the reference number indicated above.

Note that should any other instruments be required or amendments become necessary, these require separate authorisation.

Please note that UREC must be informed immediately of

- Any material changes in the conditions or undertakings mentioned in the document;
- Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research.

The student must report to the UREC in the prescribed format, where applicable, annually, and at the end of the project, in respect of ethical compliance.

UREC retains the right to

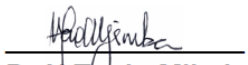
- Withdraw or amend this approval if
    - Any unethical principal or practices are revealed or suspected;
    - Relevant information has been withheld or misrepresented;
    - Regulatory changes of whatsoever nature so require;
    - The conditions contained in the Certificate have not been adhered to.

- Request access to any information or data at any time during the course or after completion of the project.

Your compliance with Department of Health 2015 guidelines and any other applicable regulatory instruments and with UREC ethics requirements as contained in UREC policies and standard operating procedures, is implied.

UREC wishes you well in your research.

Yours sincerely



Dr N Taole-Mjimba
Chairperson: University Research Ethics Committee
11 August 2022

Appendix 4*:* Frequencies and percentages for effect of cyber knowledge and cyber safety awareness

View or Opinion of first-year students	Strongly agree	Agree	Disagree	Strongly disagree
I am not ignorant of security concerns regarding smartphones	87(23)	230(60)	26(7)	6(2)
I am not fully aware of all the security risks and necessary security practices.	45(12)	218(57)	70(18)	9(2)
I never share my password or post it where others may obtain access to it	174(45)	158(41)	9(2)	5(1)
I know how to protect against 'social engineering' 'phishing' and 'cyber crime'	39(10)	155(41)	129(34)	25(7)
When away, I always lock my PC and employ my system's password protected screen saver	122(32)	190(50)	30(8)	5(1)
I am careful when opening email attachments and links	96(25)	216(56)	29(8)	6(2)
I do not use mobile applications which request for accessing your contacts, camera or location	59(15)	165(43)	109(29)	14(4)

Appendix 5*:* Frequencies and percentages for effect of cyber attitude on cyber safety awareness

View or Opinions of first-year students	Strongly disagree	Disagree	Agree	Strongly agree
It is a waste of time to change passwords because you can still get hacked	44(12)	117(31)	124(32)	32(8)
It is too difficult to remember difficult passwords; therefore I use my name or something easy to remember.	75(20)	148(39)	75(20)	19(5)
Posting pictures and bad messages online about my college students makes it anonymous and is much better than saying it to their face.	31(8)	65(17)	112(29)	108(28)
The security settings and tools slow me down and are pesky. I turn them off or disable them.	18(5)	102(27)	162(42)	32(8)
Updating my security software and Windows /Apple is too time consuming, annoying and uses up my bandwidth/ data bundle.	23(6)	129(34)	118(31)	48(13)

Appendix 6*:* Frequencies and percentage of the views of students on the measures needed to alleviate the challenges cyber threats

View or Opinion	Strongly agree	Agree	Disagree	Strongly disagree
Training and awareness campaigns	128 (33)	160(42)	16(4)	1(0.3)
Frequent secure password changes	78(20)	165(43)	53(14)	8(2)
Practising safe computing	120(31)	172(45)	6(2)	3(1)
Incorporate cyber security issues in the curriculum	71(19)	190(50)	40(10)	3(1)
Gaming for cyber security awareness	67(18)	180(47)	51(13)	7(2)
Development of cyber security policy or framework	86(23)	186(49)	27(7)	3(1)

Appendix 7: Expert interview questions

1. What are the critical success factors needed for the development of a cyber safety framework for first year university students? From literature, I identified the follow critical success factors, what is your comment on them in the development of a cyber safety awareness framework:

   -Human factors: knowledge, attitude, risk perception,

   -Attitude of the students towards passwords, trust of the internet, making downloads from sites

   -Risk awareness especially identity theft, sexting, bullying

2. What are the challenges faced by university students in terms of their cyber safety awareness?

3. What are your concerns about the initial model on cyber safety awareness? The overall factor, sub-elements and their relatedness and impact on cyber safety awareness. Are the suggested factors in line with the research objectives?

4. What theories can be included in developing the model?

5. Are the changes made to the revised model in line with the first revisions I have submitted? If not which areas need to be realigned?