**UNIVERSITY OF KWAZULU-NATAL**

# Understanding students' compliance behaviour with the information security measures within a South African university

**By**

**Sabelo Moses Masinga**

**214552237**

**A dissertation submitted in fulfilment of the requirements for the degree of Master of Commerce (Information Systems and Technology)**

**School of Management, IT and Governance**

**College of Law and Management Studies**

**Supervisor:**

Dr. Surika Civilcharran

**2022**

# DECLARATION

I, Sabelo Moses Masinga, declare that:

(i) The research reported in this dissertation/thesis, except where otherwise indicated, is my original research.

(ii) This dissertation/thesis has not been submitted for any degree or examination at any other university.

(iii) This dissertation/thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This dissertation/thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

a) their words have been re-written but the general information attributed to them has been referenced;
b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

(vi) This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

Signature:

Date: 03 May 2023

# ACKNOWLEDGEMENT

First and foremost, I would like to thank the Almighty God for blessing me with the strength to start this study and see it to completion. Moreover, I would like to extend my gratitude to my mother, Ms Masinga, for her unwavering support.

I express my deepest gratitude for the support and guidance of my supervisor, Dr Surika Civilcharran. I am very grateful for the assistance provided by virtually every single person whom I have consulted in the course of the research. I particularly must acknowledge the interest and dedication of Dr Patrick Ndayizigamiye. I would like to express great appreciation to Dr Nurudeem Ajayi for the valuable advice, guidance and supervision at the beginning of the study. This university is lucky to have such individuals, I would work with each and every one of you again in future.

In addition, my acknowledgement would not be complete without showing gratitude to my main source of my strength, my family, particularly my siblings, Anna Masinga, Zanele Masinga and Ashley Masinga. I would like to offer my special thanks to you for your unconditional love and support, Thank you. Finally, my gratitude goes Silungelo Ngcobo for the support and encouragement in the duration of the study. I am very thankful to all my friends and colleagues; it has been an absolute pleasure working with you.

# ABSTRACT

Today's organisations are continuously and increasingly being exposed to security breaches. Higher education institutions have also been affected by the increasing occurrences of security breaches. Higher education institutions' exposure to security breaches have been attributed to factors such as human error and lack of information security compliance among students. Studies have shown that students do not comply with information security policies. Hence, students, like most humans, remain the weakest link in the exposure of information and information systems to cyberattacks.

In this study, the protection motivation theory was used as the guiding theoretical framework to understand students' compliance behaviour with information security measures. This study employed an exploratory research design supported by a quantitative research approach to investigate the factors influencing students' compliance with information security measures. The data was collected using a questionnaire and was analysed using the statistical package for social science (SPSS). From a stratified sample of 376 participants, the findings indicate that Perceived Severity and Perceived Rewards have the most significant effect on student compliance with information security measures. This study further makes suggestions that may help improve compliance with information security controls within higher education institutions, such as replacing the student card system with biometric fingerprint scanners which are a more convenient method to access the university.

# Table of Content

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

CA - Coping Appraisal

F - Factor (F1, F2, F3)

FA - Factor Analysis

GTR - General deterrence Theory

ICS - Information & Communication Services

IDS - Intrusion Detection Systems

IP - Internet Protocol

IS – Information Security

KAB - Knowledge Attitude Behaviour (KAB) Model

LAN – Local Area Network

PCA - Principal Components Analysis

PMT - Protection Motivation Theory

Q - Question (Q1, Q2, Q3...)

Sig - Significance

RQ - Research Question (RQ1, RQ2, RQ3 & RQ4)

SPSS - Statistical Package for the Social Sciences

TA - Threat Appraisal

TAM - Technology Acceptance Model

TPB - Theory of Planned Behaviour

TRA - Theory of Reasoned Action

UKZN - University of KwaZulu-Natal

VPN - Virtual Private Network

Wi-Fi – Wireless Fidelity

# CHAPTER 1: INTRODUCTION

## 1.1. Introduction

The introduction chapter provides the overview of this research. The chapter presents the background and addresses the gap in the study, justification and significance for conducting this research. Moreover, this section also introduces the problem, questions, goal, methodology of the study and restrictions the study encountered.

## 1.2. Background and Gap of the Study

Parsons et al. (2014) argue that many previous studies investigating cybersecurity issues often ignore the human dimension associated with cybersecurity breaches. They further deduced that numerous academic research has only explored one aspect of security. Case in point, Stanton et al. (2005) carried out their study only about password-related behaviour and Siponen et al. (2010) researched intentions to comply with information security policy. Parsons et al. (2014) stated that not one of these research aims to find comprehensive and all-inclusive information on information security. Mohammed (2015) also argues that the existing studies have not explicitly identified all the elements that have major effects on the adoption or improvement of a data security compliance mindset. Therefore, this research will not focus on one aspect of information security, but it will address most of the known and frequently performed mistakes in an institution.

These studies have been criticised due to inadequacy and flaws in their methodology, questionnaires, and data analysis (Guillot & Kennedy, 2007). Anderson and Barton (2012) pointed out that these research papers experienced sampling bias which causes under-addressing or over-addressing of information security problems. Herath and Rao (2009a) claim that these studies are usually carried out with an assistance of an information security professional. Although they uncover existing problems and solutions to secure institutional data, this does not represent the perspective of the majority or common end-users of the university systems. Subsequently, this study will solely focus on the common end-user i.e., students that will represent the whole population adequately.

According to Parsons et al. (2014) and Vestad (2022), an increasing number of literature utilise the present behavioural models in the data security field. For example, the Theory of Planned Behaviour (TPB), General deterrence Theory (GTR), Technology acceptance model (TAM), Health Belief Model, Knowledge Attitude Behaviour (KAB) Model, and Extended Parallel Process Model. Karjalainen (2011) adds that these behavioural models

are centred on validation or verification which might raise a biased point of view. Furthermore, Vestad (2022) states that TPB and TAM are more generic frameworks that do not prioritise threat appraisal as a primary determinant in security behaviour. In addition, GTR is more suitable for non-voluntary behaviour studies as this research investigates voluntary behaviour.

Maddux and Rogers (1983) and Vestad (2022) define PMT as the individual's intention to engage in a protective behaviour (such as quitting smoking) based primarily on a threat appraisal that considers the perceived seriousness of the threat and one's vulnerability to the threat. In addition to a coping appraisal that considers the perceived effectiveness of the response and the likelihood of success. Unlike TPB, TAM and GTR, PMT prioritises threat appraisal and is a voluntary behaviour-based theory. Moreover, Mou et al. (2022) conducted a meta-analysis of 92 published studies that utilised PMT. According to Mou et al. (2022), the findings provided strong support for Response Efficacy and Self-efficacy as most significant predictor of protection motivation in information security. Findings from a study conducted by Sommestad et al. (2015) indicate that PMT seems to explain information security behaviour better if the threat and coping methods are concrete or specific. Additionally, 61 of 67 empirical research endorse the use of PMT in an information security context (Haag et al., 2021). In the context of this study, it was determined that the constructs of the protection motivation theory (PMT) were the most pertinent and fitting for the research objectives.

### 1.3. Justification

This study needs to be carried out as it will examine and make recommendations regarding ways in which the existing data security culture can be improved. Furthermore, the study could assist in educating, mitigating security breaches and securing the university's data. Failure to conduct this study will lead to a continuous cycle of students neglecting security seriousness, and the university will continue to have security breaches.

### 1.4. Research Problem

According to Hina and Dominic (2017), security breaches in higher education institutions have increased at an alarming rate in recent years and continue to increase with the growth of technological innovations. For example, the University of KwaZulu-Natal student e-mail accounts faced security breaches numerous times at the beginning of 2018 due to

weak passwords and a lack of information security compliance among students as shown in Appendix B (Information & Communication Services, 2018). Furthermore, Information & Communication Services (2022) claims that 80% of data breaches that occurred in 2019 and 2020 were a result of compromised passwords (Appendix B). Parsons et al. (2010) argue that humans are the weak point in enforcing information security controls and measures. Thus, fostering an information security culture of compliance within an organisation is very crucial in order to deal with cyber threats and risks. Thus, this research primarily investigates factors that may influence compliance with information security measures at the University of KwaZulu-Natal in Pietermaritzburg and Westville campus from a student's perspective. Identifying such factors is a stepping stone towards adopting strategies that may lead to greater compliance and therefore mitigating risks associated with information security breaches.

### 1.5. Research Questions

The following research questions were constructed from the research problem to aid in accomplishing the research's objectives. Protection Motivation Theory has two main constructs, namely, Threat Appraisal and Coping Appraisal. Coping Appraisal refers to the psychological and behavioural responses that individuals use to manage and adapt to stress or challenging situations. Threat Appraisal is a concept in psychology that refers to the process of evaluating and assessing the perceived severity and likelihood of a potential threat or danger.

1.5.1. How compliant are students with the existing information security measures currently in place within the university?

1.5.2. What are the effects of threat appraisal on students' compliance with the information security measures within the university?

1.5.3. What are the effects of coping appraisal on students' compliance with the information security measures within the university?

1.5.4. What are the challenges faced by students in their compliance with the information security measures within the university?

### 1.6. Research Objectives

The research objectives of this study are the following:

1.6.1. To investigate how compliant students are with existing information security measures currently in place within the university.
1.6.2. To identify threat appraisal effects on students' compliance with the existing information security measures in place within the university.
1.6.3. To identify coping appraisal effects on students' compliance with the existing information security measures in place within the university.
1.6.4. To identify the challenges that may hinder students from complying with the information security measures in place within the university.

### 1.7. Significance of the Study

This research identifies the influences that may encourage students to comply with data security culture; based on those factors, the study can suggest or recommend strategies that can be used to encourage students to comply with data security measures in place. If the suggestions and recommendations are taken into consideration, then they could aid in minimising the occurrence of security breaches.

The study uses the Protection Motivation Theory. Subsequently, this research will contribute to the body of knowledge by applying the constructs of the theory to analyse students' behaviour with the data security measures. Findings from this study will assist in discovering what needs to be implemented to enable the improvement of information security culture in the context of an institution.

### 1.8. Research Limitations

One of the limitations of this study is that it has been conducted at a single institution, which may restrict the generalizability of the findings. Specifically, the results of the study may only be relevant and applicable to the university in question (i.e. UKZN), rather than being able to be extended to other institutions or settings. This could potentially impact the validity and usefulness of the research. Time was another constraint for this research. Nevertheless, the researcher began data collection as soon as the second semester commenced.

### 1.9. Concluding Remarks

This chapter introduced the concept of information security, addressed the gap and the background of this study, and outlined the significance and justification for carrying out this research. This chapter also introduced the research problem, question, objectives,

methodology, and the restrictions of this study the researcher came across. The following chapter provides the literature review based on the above concepts.

# CHAPTER 2: LITERATURE REVIEW

## 2.1. Introduction

The literature focuses on research regarding instilling an information security compliance culture in institutions. The literature further discusses the human factor associated with information security compliance. Moreover, the literature reviews the compelling factors that could aid in creating or improving the information security culture (Masrek, 2017). This literature also discusses the role of these factors (i.e. information security awareness programs, security policies, and assessments) in improving the information security culture of compliance (Mohammed, 2015). Additionally, this literature highlights the theoretical frameworks that have been implemented in prior studies that investigated cybersecurity compliance.

## 2.2. Human Factor in Data Security

Ali et al. (2021) and Ghazvini and Shukur (2017) stated that 95% of information security breaches are a result of human errors. Furthermore, Ghazvini and Shukur (2017) stated that technology flaws are not the major sources of breaches at any organisation or even an educational institution, but the main origin of these breaches is from the employees or students' mistakes. Hence, information security cannot be addressed from a technical point of view alone, but from a non-technical stance as well (e.g. students' awareness and conduct towards information security compliance).

Other authors (Ahmed et al., 2012; Ali et al., 2021) further pointed out that while solutions such as anti-virus software, VPNs, and firewalls are necessary and beneficial, these technologies cannot be relied upon alone to combat security breaches. Hence, the students become the frontline defence. Conteh and Schmick (2016) state that students are the main focus of data security within an institution since the strategies employed by malicious actors to penetrate systems rely heavily on human mistakes. Careless errors made by students expose unsecured network channels leaving entire systems unprotected. Consequently, human errors tend to cause more damage than technological vulnerabilities (Waly et al., 2012).

Cancino-Montecinos et al. (2020) and Ahmed et al. (2012) explained that mistakes could be distinguished by situational (dependent on a set of circumstances or state of affairs) and psychological (associated with the mental and emotional state of a person) characteristics. In addition, Ahmed et al. (2012) recognised three categories of errors:

"skilled-based", "rule-based", and "knowledge-based". Skill-based mistakes occur unknowingly and automatically in a person's daily work routine. Furthermore, this category of mistakes is usually known as slip-ups or inadvertent acts. Algarni et al. (2020) further stated that rule-based mistakes occur once there is a mandatory change to saved rules and it is typically automatic operations that cause them. Moreover, the user may use previously memorised rules, meanwhile, the rules have been modified therefore causing an error. Algarni et al. (2020) and Ahmed et al. (2012) added that knowledge-based errors occur after repeated failures and there is no existing solution. The majority of these errors tend to happen in the skilled-based category. (Ahmed et al., 2012; Algarni et al., 2020; Gümüşbaş et al., 2020).

### 2.3. Improving Data Security Awareness Training Programmes

Ghazvini and Shukur (2017) state that information security awareness is lacking amongst many students. However, data security awareness training programmes could be utilised to mitigate human mistakes (Bada et al., 2019; Shahri et al., 2012). Yet, in most cases, university management neglects to teach students about the students' important role in maintaining a security compliance culture in the institution (Hale & Brusil, 2007; Hina et al., 2019).

In accordance with Shaw et al. (2009) and Hina et al. (2019), security awareness is a person's understanding of how important data security is, what exactly they are supposed to do, and the manner in which they apply what they have learnt about data security procedures to ensure the safety of the institution. Shaw et al. (2009) followed by naming certain behaviours that are capable of endangering the institution. Among these actions is the sharing of institution's computer resources with non-members. Furthermore, exploiting the institution's computer resources for the individual's benefit (such as internet shopping) and opening unknown malicious emails and their attachments. (Hina et al., 2019; Shaw et al., 2009).

Student's awareness contributes significantly to information security effectiveness (Ghazvini & Shukur, 2017). The research acknowledged that security awareness training programmes might provide students with the necessary skills and knowledge which is important for reducing the number of data security breaches (Bada et al., 2019; Waly et al., 2012). Ali et al. (2021) and Lacey (2010) also mentioned that awareness programmes are a useful and potent tool for minimising security breaches. Thus, students will be aware

of potential threats to information security and realise that their choices carry repercussions. It is essential to raise students' awareness in order to keep sensitive data secure (Bakar et al., 2021; Eminağaoğlu et al., 2009).

### 2.4. Information Security Measures and Control

According to Bakar et al. (2021) and Chan and Mubarak (2012), security specialists have been emphasizing the vulnerability of data and computing resources in higher education institutions. Subsequently, they recommended that security controls and measures in these institutions should be current and occasionally revisited to keep abreast of the propelling dangers and security breaches. Haeussinger and Kranz (2013) and Wheelus and Zhu (2020) claim that the security controls and measures put in place in higher education institutions are intended to manage or oversee the technical problems such as malware, virus infections through faux sites, and malicious programs. However, human carelessness associated with the misuse of resources and data is frequently disregarded. Security measures should be incorporated into an individual's daily activities (Daneshmandnia, 2019; Sun, 2016; Wheelus & Zhu, 2020). The following proposed security measures should build a dependable and safe environment (Daneshmandnia, 2019; Sun, 2016; Wheelus & Zhu, 2020).

#### 2.4.1. Firewalls

Firewalls are software and hardware devices that isolate local networks from external networks. Moreover, firewalls prevent unauthorised access to the internal network. This ensures that only data that has been checked for accuracy and safety can be accessible. Encrypting, decrypting, compressing, decompressing, and authorizing, are some of the functionalities that are built into firewalls during their development (Al-Haijaa & Ishtaiwia, 2021). Therefore, an institution's network security significantly improves when it is equipped with a firewall. It can be argued that firewalls have played a crucial role in improving the security networks in a university (Sharma et al., 2021). From a university perspective, firewalls have shown to be effective in protecting against a wide range of network attacks (such as unauthorized access, malware and viruses, network attacks), while also allowing authorized communications (Al-Haijaa & Ishtaiwia, 2021; Sharma et al., 2021).

### 2.4.2. Intrusion Detection Systems

Intrusion Detection Systems (IDS) are utilised to identify potentially malicious activities and compliance violations within the network. The system reports malicious activities when they are discovered. Other systems respond to malicious activities by restricting the traffic from the originating IP address. When hackers manage to penetrate the firewall, intrusion detection systems are incredibly helpful (Alsaedi et al., 2020). Mendonça et al. (2021) claim that IDS have greatly contributed to the security effectiveness of university networks. One of the key contributions of IDS to security effectiveness in a university setting is their ability to detect and alert on known and unknown threats (Gümüşbaş et al., 2020). Another important contribution of IDS in a university setting is their ability to monitor and protect the various devices that are connected to the university's network. This is especially important in a university setting where the number of connected devices and users is constantly growing. With the increasing number of students, faculty, and staff connecting to the university's network, the risk of security breaches and cyber-attacks also increases (Gümüşbaş et al., 2020; Mendonça et al., 2021). The use of IDS is a necessary step in ensuring the safety and integrity of a university's network and its sensitive information (Mendonça et al., 2021).

### 2.4.3. Data Encryption

Encrypting information is among the best strategies for data protection. Data encryption is the process of converting information into a secretly encoded message (Wen et al., 2021). Moreover, data encryption provides institutions a means of verifying the authenticity and integrity of data. Encryption algorithms use digital signatures to verify the authenticity of a message and to detect any tampering with the message. This is important for universities, as it helps to ensure that the information they are using is accurate and has not been altered in any way state (Prajapati & Shah, 2022; Zimba et al., 2018). Another contribution of data encryption to security effectiveness in a university setting is its ability to protect data at rest. This helps to prevent unauthorized access to the information, even if the device is lost, stolen, or compromised. This is important for universities, as the loss of sensitive information can have severe consequences, including damage to the university's reputation, finances and potential legal liability (Prajapati & Shah, 2022; Zimba et al., 2018).

### 2.4.4. Virtual Private Network

A virtual private network, or VPN, is one of the most effective technologies for protecting student's privacy online, as the student's data connection is encrypted and concealed (Empey & Latto, 2022). Furthermore, a VPN allows students to connect to private networks across public networks. For instance, when a student is away from the university and required to connect to the university's network, this is possible with the use of a VPN.

### 2.4.5. Backup and Data Restoration

Backup and data restoration are among the essential parts of data security controls. It should be standard practice to back up data containing sensitive or vital information regularly. In the event that information is accidentally deleted or becomes corrupted, the backups are able to retrieve the most recent uncorrupted data (Prajapati & Shah, 2022). Individuals need to have training in this particular area and be reminded frequently to put it into practice. In the context of a university, backup and data restoration play a significant role in enhancing security by mitigating the risk of data loss (Zimba et al., 2018). Universities often handle large amounts of valuable and sensitive information, such as research data, student records, and financial information. This information is critical to the daily operations of the university and its continued success. By regularly backing up this information, universities can ensure that they have a copy of the data that can be used to restore it in the event of a data loss or data breach (Thomas & Galligher, 2018).

### 2.4.6. Authentication

In a university setting, authentication plays a crucial role in securing the network. Authentication serves as the initial checkpoint since it controls who accesses the university network, therefore, it is among the most important steps in a data security process. Through student login credentials or a biometric system, authentication is used to verify authorised students to access the system. Furthermore, authentication manages authorization for resources within the network. In order to ensure the security of the system, students are urged to update their login credentials on a frequent basis (Khan et al., 2020; Prajapati & Shah, 2022; Zimba et al., 2018).

## 2.5. Enforcing Information Security Policy

According to Hamid and Zeki (2014), institutions document their security requirements as security policies and convey them to students via electronic mail. Consequently, the

effectiveness of information security policies in institutions is debatable since students are not frequently included in security awareness agendas, meetings, and teachings. Cheng et al. (2013) emphasized that there is an insufficient inspection of students' compliance with information security policies thus propelling unawareness regarding imperative action that has to be taken against security breaches. Consequently, increasing security breach occurrences. During awareness educational programmes, an institution's internal policy regarding data security is an important factor to consider (Ghazvini & Shukur, 2017). Therefore, discussions pertaining to internal policies aid students in better understanding the importance of data security and obtaining the knowledge necessary to prevent data breaches (Ghazvini & Shukur, 2017).

### 2.5.1. Policy Awareness

It is believed that having knowledge about policies is among the most important aspect in assuring the efficiency of data security, and the success of data security depends on the individuals with that knowledge (Knapp and Ferrante 2012). Therefore, Knowledge sharing of policies must not be overlooked. By establishing clear guidelines for secure practices, policy awareness helps to reduce the likelihood of security incidents and data breaches at the university. In a university environment, policy awareness can play a critical role in ensuring the protection of sensitive academic and research data, as well as ensuring the privacy and confidentiality of student and faculty information (Aldawood & Skinner, 2019; Bada et al., 2019). This can be achieved through regular training and education programs that educate students, faculty, and staff on the importance of secure practices, as well as the consequences of policy violations (Aldawood & Skinner, 2019; Bada et al., 2019). In addition to reducing the risk of security incidents, policy awareness can also help to improve the overall security posture of a university by promoting a culture of security. By emphasizing the importance of security and encouraging the adoption of secure practices, policy awareness can help to create a security-conscious environment where individuals are more likely to be vigilant and proactive in protecting sensitive information and systems (Aldawood & Skinner, 2019; Bada et al., 2019).

### 2.5.2. Policy Enforcement

According to Ghazvini and Shukur (2017), institutions must assume responsibility for enforcing the institution's security rules. Further adding that institutions are responsible for ensuring that students have access to approved education programmes for a successful data security culture. For instance, institutions must make sure that data security

programmes are seamlessly integrated into the student's regular routine. In addition, it is important that students be informed about the repercussions of any data breach that occurs.

### 2.5.3. Policy Maintenance

The institution is solely responsible for keeping security policies up-to-date, and it is crucial to monitor and evaluate students' growth and cognizance of the data security (Ghazvini & Shukur, 2017). Moreover, an institution is responsible for ensuring that the policies are accurate and still secure the institution's data.

## 2.6. Information Security Culture

In accordance with Ngo et al. (2009), information security culture consists of two components: "information security" and "culture". The term "information security" describes methods employed by an organisation or institution to ensure the safety of data, whether it be intellectual property, physical files, or data in transit. Bada et al. (2019) state that culture is a complex concept, and every organisation or institution has its security protocols that are put into practice and eventually become ingrained in the students mindset. Information security culture should strive to protect institutions' data and encourage individuals to adopt a security compliance mindset (Aldawood & Skinner, 2019; Bada et al., 2019).

For instance, ensuring users make it a habit to frequently change passwords. Subsequently, users would consider frequently changing passwords a normal practice. Schein (2009) defines an institutional culture as a phenomenon which develops and alters after a while to some degree, information security policies may be changed or composed by the board of directors.

According to Ghazvini and Shukur (2017) the importance of data security has prompted institutions to develop rules and protocols to safeguard their assets. This is because security is a growing concern in businesses and institutions, particularly in the healthcare industry where reliable data is essential for making medical decisions. For this reason, these industries must adopt a better mindset of data security in order to protect themselves. Therefore, these sectors need to acquire superior information security culture to safeguard their data. Two to three percent of an institution's yearly income is lost due to data security and breaching occurrences and it is primarily because of human conduct (Ali et al., 2021; Ghazvini & Shukur, 2017; McIlwraith, 2006).

### 2.7. Improving Information Security Compliance Culture

Mohammed (2015) emphasizes that a security culture must strengthen every aspect of the institution's practices so data security begins to be an inherent element of a student's day to day deeds and by doing so, consequently improves the information security culture of compliance. Ngo et al. (2009) and Aldawood and Skinner (2019) claim that improving information security culture implies improving the state of mind, behaviours, beliefs, and values with a common goal of a consistent conduct. Furthermore, creating awareness of privacy amongst students and employees, acquiring a compliance habit of making security a second nature and applying it to their day-to-day endeavours can help improve information security culture.

Further suggestions to improve an information security culture of compliance are: support and dedication from the top management, well thought out and constructed security policies and instructions are the backbone of an institution, offer basic information security awareness training, students' duties and obligations should be plainly outlined, remain well-informed of present and altering laws and regulations, utilise the available technologies and software programs, and review and analyse the security efforts made over a period of time (Aldawood & Skinner, 2019; Bada et al., 2019; Ngo et al., 2009).

An institution carried out a study in which information security culture was assessed four times after eight years across 12 countries. Furthermore, the study was conducted in order to develop a usable model for data security culture that works well (da Veiga & Martins, 2015). The authors further stated that the study intended to investigate information security culture enhancements, recognize changes, and determine long-term patterns. In addition, the study intended to demonstrate how data security culture enhances by monitoring. The study proved that assessing awareness and training instils an effective information security culture in the long run.

### 2.8. Student Compliance in Information Security

Hina and Dominic (2020) defines Student Compliance in information security as the adherence of students to the rules and regulations set by a school or educational institution to protect sensitive information and maintain the security of the network and systems. This can include policies on the acceptable use of technology, password protection, and data privacy. Furthermore, ensuring student compliance is important to prevent security breaches and protect the integrity of the educational institution's information (Hina &

Dominic, 2020). Bauer and Bernroider (2017) and Bauer et al. (2017) state that institutions implement information security policies in order to safeguard the institution's resources. However, when end-users fail to comply with these policies or demonstrate a lack of interest in adhering to them, the institution's efforts to implement these policies become futile (Bauer et al., 2017; Herath & Rao, 2009b).

Muhammad and Naeem (2018) explored the factors that influence student compliance with information security policies in higher education institutions. The study found that students were more likely to comply with information security policies if they believed the policies were fair (Murphy et al., 2009), if the policies were clearly communicated (Feng et al., 2019), and if there were consequences for non-compliance (Puhakainen & Siponen, 2010). Additionally, the study found that students who had a higher level of computer Self-efficacy were more likely to comply with information security policies. Furthermore, research has shown that the design of information security policies can also affect student compliance, with policies that are perceived as more restrictive being less effective in promoting compliance (Ormond et al., 2019; Steinbart et al., 2016). Moreover, D'Arcy and Greene (2014) discovered that end-user satisfaction has an impact on their intention to comply with security measures. Other studies found that a well-designed security awareness campaign can be effective in promoting student compliance and that the use of multiple communication channels can increase the effectiveness of the campaign (Alharbi & Tassaddiq, 2021; Puhakainen & Siponen, 2010). Despite the crucial nature of information security policies in institutions, there is a recurrent tendency among users to disregard these policies or fail to comply with their institution's information security policies (Bauer & Bernroider, 2017; Bauer et al., 2017; Hina & Dominic, 2016).

Compliance with information security policies institutions has been somewhat under-examined, with a lack of validated evidence (Hina & Dominic, 2016). Hina and Dominic (2016) continue to claim that the latest studies conducted in institutions have emphasized the need for the development of an inclusive framework for compliance with information security policies to mitigate the threats in vulnerable institutions. Furthermore, research has also revealed that insider maltreatment of institutional resources is a significant threat to institutions' security. Therefore, it is necessary to examine end-users' perceptions regarding compliance with information security policies. Bauer et al. (2017) state that the perception of threats associated with information systems is a crucial factor in determining compliance. Moreover, management often perceives the unintended non-

compliance of end-users as the primary cause of information security incidents. Conversely, end-users tend to identify external threats from hackers and the internet as the most significant information security threats, and do not recognize their own actions posing any potential threat to the institution (Bauer et al., 2017).

### 2.9. Challenges Towards Student Compliance in Information Security

Student compliance issues can manifest within the context of a university setting as a result of misconceptions held by members of the university. These misconceptions may include a lack of comprehension and awareness regarding the severity of the threat and its impact on shareholders, an underestimation of the probability of a security breach occurring, or a belief that security measures are being actively managed by others. Furthermore, it has been observed that noncompliance with security protocols can be attributed to a phenomenon referred to as security illusions, where individuals fail to implement necessary security measures under the assumption that others are fulfilling such obligations when in actuality they are not (Kyobe, 2010; Shambabi et al., 2021). The authors conducted studies of compliance with security requirements within the institutions and discovered a substantial disparity between desired and actual awareness pertaining to security threats. The authors attributed this discrepancy to the abstract nature of security and the low perceived level of threat among members of the institution (Kyobe, 2010; Lane, 2007; Shambabi et al., 2021).

Chan and Mubarak (2012) and Hina and Dominic (2016) conducted research investigating the level of awareness pertaining to information security among end-users of educational institutions and findings revealed that it was generally inadequate. The study emphasized the need for enhanced security awareness strategies to cultivate a culture of security compliance and effectively mitigate information security breaches. Shambabi et al. (2021) argue that the majority of non-technical end-users possess minimal knowledge of the existence of any information security policies within their institution. This observation implies that there is a prevalent deficiency of awareness pertaining to information security among these individuals. Additionally, Shambabi et al. (2021) study suggests that despite the presence of information security policies, compliance among the majority of non-technical end-users is inadequate.

Shambabi et al. (2021) and Kyobe (2010) conducted a study to investigate the major challenges towards student compliance, the study's findings revealed significant

shortcomings in the planning and execution of security compliance policies, a lack of knowledge and understanding of the university's information security policies, a lack of information security awareness, and an absence of decision-makers participation in the development and employment of information security policies. The authors added that individuals with a narrow understanding of information systems tend to neglect the potential hazards and ramifications of system malfunctions. Furthermore, the authors argue that decision-makers who perceive security risks to be insignificant are unlikely to allocate resources towards mitigating those threats. As a result of this limited understanding, ineffective coping mechanisms may be implemented in response to such situations (Kyobe, 2010; Shambabi et al., 2021; Tribbensee, 2003).

In addition, Ormond et al. (2019) state that individuals that are emotionally overwhelmed negatively are unlikely to adhere to information security policies. Prior research has revealed that even seemingly minor changes like interface design for changing passwords can have an impact on people's security compliance behaviour (Ormond et al., 2019; Steinbart et al., 2016).

### 2.10. Overall Summary

Hina and Dominic (2017) articulated that the combination of computer software programs and behavioural controls creates a security culture inside an institution. Nevertheless, higher education institutions significantly depend on these computer software programs while neglecting the human factor. Therefore, neglecting human compliance to information security measures may result in the re-occurrence of security breaches. This literature discussed the information security culture and proposed ways on how to improve it. It also reveals the gaps in the information security compliance culture in the research (Parsons et al., 2014). This literature also discussed the role information security tools and preventative measures. Furthermore, the literature discussed the factors of improving information security culture of compliance (Alnatheer, 2015). The literature focused on student compliance in information security and discussed the importance of preventing security breaches. Furthermore, the literature revealed that students are likely to comply with information security policies if there were consequences for non-compliance and the students who had a higher level of computer Self-efficacy were more likely to comply with information security policies compliance (Ormond et al., 2019; Steinbart et al., 2016). In addition, the literature revealed challenges towards student compliance such as, lack of awareness of information security policies.

## 2.11. Theoretical and Conceptual Framework

### 2.11.1. Theoretical Framework

According to Masrek (2017) and Chenoweth et al. (2009), due to the increase in instances of data breaches, there's a developing enthusiasm amongst academics to research about data security culture. Subsequently, academics utilised and created several frameworks for evaluating and creating an information security culture. These frameworks include the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1977), the Technology Acceptance Model (TAM) (Davis, 1989), and the Theory of Planned Behavior (TPB) (Ajzen, 1991). However, Chenoweth et al. (2009) state that most of these frameworks have not been utilised for studying protection behaviours. In accordance with Bulbulia and Maharaj (2013), information system theories such as TAM, focus mainly on the adoption of technology by end-users thus deeming them to be unfitting for this study.

According to Floyd et al. (2000) and Chenoweth et al. (2009), the information security field will benefit more from using frameworks from other disciplines. Specifically, the health sector has applied and refined the Protection Motivation Theory (PMT) for many years to better understand compliance intention. Ng et al. (2009) state that protective security behaviour and preventive healthcare behaviour are quite similar. For example, protective security behaviour would entail a strong password to prevent unwanted account access. With regard to preventative healthcare behaviour, one example is to refrain from smoking in order to avoid developing lung ailments. Ng et al. (2009) defines protective security behaviour as a practice that reduces the likelihood of security incident. Jayanti and Burns (1998) defining preventive healthcare as actions that will prolong a person's lifespan or reduce the risk of diseases. Therefore, both include taking action to prevent an undesirable situation (Bulbulia & Maharaj, 2013)

### 2.11.2. The Protection Motivation Theory

The Protection Motivation Theory (PMT) was suggested by Rogers in 1975 as shown in Figure 2-1 (Rogers, 1975). According to Bulbulia and Maharaj (2013) and Rogers (1975), PMT explains the effect of fear on behaviour and explicitly illustrates how people are motivated to react and protect themselves from harm or threats which is called a fear appeal. Chenoweth et al. (2009) state that change in behaviour is not only said to be an outcome of feeling fear, a protective motive also arising from the cognitive appraisal. Moreover, Vance et al. (2012) states that people utilise a cognitive process to think about

their reaction to threat, which is "*Threat Appraisal (TA)"* and "*Coping Appraisal (CA)*" and invokes a protective behaviour.

Threat Appraisal (TA), also known as fear appeal, defines a threat's perception. It contains three constructs, namely; (1) Perceived Severity (i.e. size or degree of the threat), (2) Vulnerability or susceptibility (i.e. the probability of the threat to happen), and (3) Rewards or benefits (i.e. any internal or external motivation for staying with the undesirable behaviour) (Chenoweth et al., 2009; Rogers, 1975).

Coping Appraisal (CA) defines the skill or means of a person to cope with a threat. It is made up of three constructs, namely, (1) Self-efficacy (i.e. the person's confidence in their capability to take protective measures), (2) Response Efficacy (i.e. perceived profits of eliminating the threat), and (3) Response Cost (i.e. costs or obstacles that hinder the adoption of this behaviour). Witte (1992) declared that threat appraisal triggers fear, this, together with coping appraisal prompts protection motivation (PM) and the overall aim of PMT is to adopt a protective behaviour.

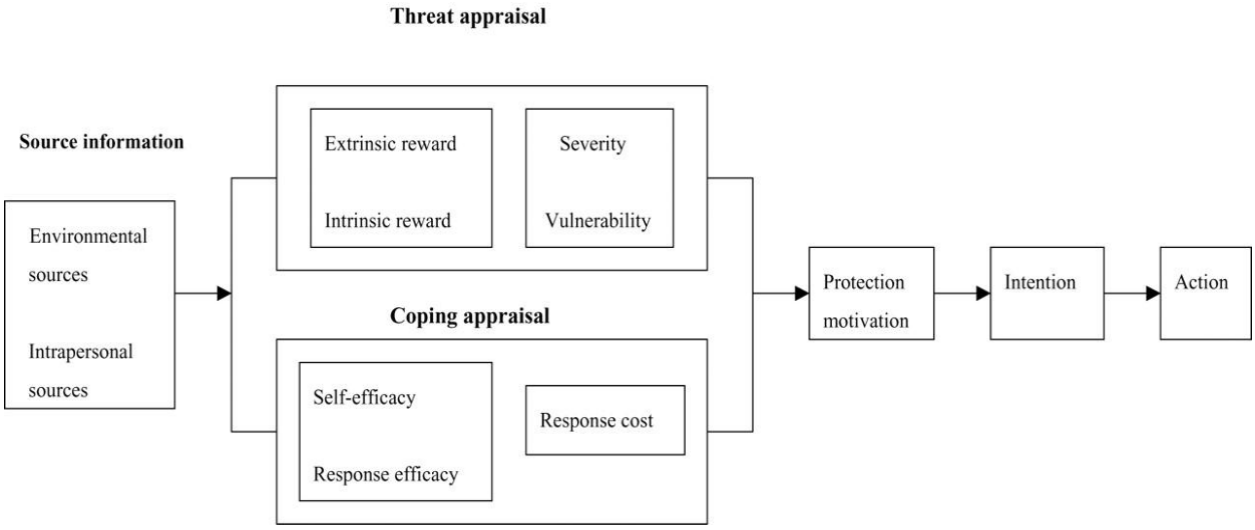



***Figure 2-1: The Protection Motivation Theory (***Wu et al., 2005, p. 128***)***

According to Floyd et al. (2000), the Protection Motivation Theory has been traditionally implemented within the context of an individual's well-being. A meta-analysis research conducted on PMT classified six significant groups that used (PMT) namely; cancer avoidance (17%), workout/food plan (17%), cigarettes usage (9%), alcohol intake (8%), AIDS anticipation (9%) and compliance to clinical-treatments (6%).

Apart from personal physical fitness studies, the Protection Motivation Theory usage has extended to different regions. Specifically, academics began to focus on information security and implemented PMT in their research in 2000. The overall concept has been to apply threat or fear as security guidelines to encourage protection behaviours inside an institution (Herath & Rao, 2009b). While numerous authors have made substantial contributions to the evolution of the Protection Motivation Theory, additional research is necessary to further study and expand upon the theory, adding to the current body of knowledge (Boss et al., 2015). According to Boss et al. (2015), certain studies do not utilise all of the Protection Motivation Theory's constructs. For instance, Vestad (2022) deemed Self-efficacy as less pertinent in the research and excluded the Self-efficacy construct. Whilst Siponen et al. (2014) did not incorporate Response Cost construct and Johnston and Warkentin (2010) omitted both the Perceived Reward and Response Cost constructs in their research. Furthermore, the authors indicated that they did not use fear appeal in their research and that most of their studies concentrated on behaviour alone and excluded security behaviour (Boss et al., 2015). Therefore, this study will address this by ensuring to utilize all the constructs of PMT, fear appeal and focus on security behaviour.

### 2.11.3. The Conceptual Framework

The research utilised PMT and adapted it to understand students' compliance behaviour with the information security measures that exist within the university. The adaptation of PMT will be to test students' behaviour, intention, and motivation to comply. The conceptual framework shown in Figure 2-2 is what the researcher intends to apply to this research. The conceptual framework is adapted from the theoretical framework presented in Figure 2-1. The researcher utilised the constructs of the theoretical framework and adapted the constructs to this study.

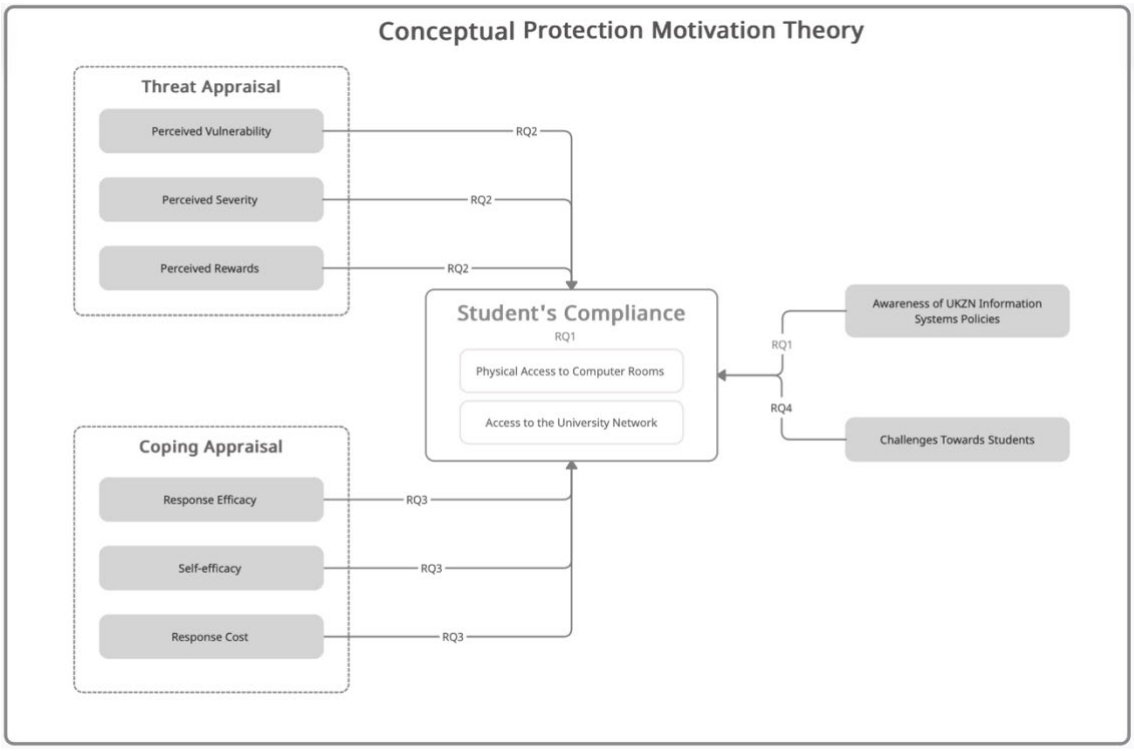



***Figure 2-2: Conceptual Protection Motivation Theory (***Wu et al., 2005, p. 128***)***

Threat Appraisal prompts individuals to assess the seriousness of an incident, the possibility of an incident occurring, and the consequences of allowing the incident to occur. Within the scope of this research, TA is utilised to investigate if the students understand the magnitude of a security breach, the likelihood of a security breach occurrence and if the students understand the consequences of a security breach.

Meanwhile, Coping Appraisal is the skill or means of an individual to cope with a threat. Within the scope of this research, CA is utilised to investigate if the students believe that they are capable of competently taking protective measures on their own against the information security breach, investigate if students believe that there are benefits of taking protective measures against security breaches, and identify reasons that hinder the students from taking protective measures.

Student Compliance refers to the extent to which students follow the rules, regulations, and guidelines related to information security. This construct is an important factor in understanding information security in an educational setting. There are two Student Compliance constructs, namely, Physical Access to Computer Rooms and Access to the University Network. Student Compliance constructs are adapted to the protection

motivation theory (PMT) framework in order to better understand the factors that influence student compliance behaviour. Moreover, by adapting Student Compliance as a construct within the PMT framework, the researcher can examine how students evaluate and assess the perceived threat and their own susceptibility to information security threats, as well as their perceived ability to cope effectively with these threats. PMT prompts individuals to engage in threat appraisal when they are confronted with a potential threat, and this appraisal process influences their motivation to take protective actions. Through analysis, the researcher can identify factors that are significantly associated with greater or lower levels of student compliance.

Challenges Towards Student Compliance is also adapted in the conceptual framework in order to better understand the barriers and obstacles that prevent students from complying with rules, policies, and guidelines pertaining to information security. This construct is deemed to be of significance as it will aid in the identification and addressing of the challenges that contribute challenges student compliance at the university. The construct will aid in examining challenges such as a lack of understanding of the importance of information security, a lack of awareness of university policies, or the complexity of security measures. The outcome of the study can then be utilised to develop strategies aimed at mitigating these challenges and promoting information security at the university.

### 2.12. Conclusion

Chapter 2 presented a review of the relevant literature on the human aspect of information security in higher education institutions. The study emphasized human negligence as a significant challenge in ensuring information security compliance in universities. The literature also explored various information security measures and controls, such as firewalls, IDS, data encryption, VPN, backups, and authentications that have been suggested in previous studies to mitigate security threats at universities. Furthermore, the significance of information security policies was emphasized in the literature review. The study also analysed the information security culture and identified gaps in the current understanding of the information security compliance culture. Additionally, the literature explored the factors that contribute to improving the information security culture of compliance. Furthermore, the literature introduced the construct of student compliance and the challenges associated with it. Finally, the literature review presented the theoretical frameworks that have been adapted from PMT.

# CHAPTER 3: RESEARCH METHODOLOGY

## 3.1. Introduction

Chapter two provided the literature review as well as the framework of the research. This section presents the research design and approach utilised in this research. Furthermore, it presents the location of the research, targeted population, sampling process, sample size, sampling strategies, data collection methods, quality control, and data analysis used in this study. Additionally, the ethics were upheld within the study.

## 3.2. Research Design

The research utilised a descriptive research design to achieve the study's objective. This is because the aim of this study is to thoroughly inspect students' behaviour towards information security compliance. According to Bhattacherjee (2012), this research design is appropriate to apply to a known phenomenon. As stated in the previous chapters, this is a known phenomenon. The goal of the descriptive research design is to answer the "what" and "how" questions related to the characteristics of a phenomenon (Apuke, 2017).

Experimental designs establish cause-and-effect of relationships and manipulate one or more independent variables to determine their effect on a dependent variable, while descriptive designs only observe and describe the characteristics of a population or phenomenon (Bloomfield & Fisher, 2019; Pandey & Pandey, 2021). Explanatory research designs look for causes of the phenomenon, allowing the researcher to identify the underlying mechanisms and understanding how it works (Casula et al., 2021). Diagnostic designs are focused on identifying the presence or absence of a certain condition through tests or measurements (Joshi, 2019). Lastly, the researcher took feasibility into account when choosing the design. Alternative designs such as experimental, explanatory or diagnostic designs may require more resources, such as time, money and specialized equipment, which may not be available or make them less feasible to conduct (Pandey & Pandey, 2021). The descriptive design may be less resource-intensive, making it more feasible to conduct the study (Pandey & Pandey, 2021).

This research used Protection Motivation Theory suggested by Rogers (1975). The researcher selected a descriptive research layout since the research aims to present a clear

view of students' perceptions of adopting an information security culture of compliance. The researcher utilised the statistical analysis program (SPSS) to attain numerical results for ease of interpretation (Shields & Rangarajan, 2013).

### 3.3. Research Approach

The objective of this research was achieved by employing a quantitative research methodology. This is because the research seeks to provide an explanation of a phenomenon by collecting numerical information through a questionnaire and utilise statistical procedures for analysis (Muijs, 2010). Moreover, as this research deals with a large sample and examines the associations between dependent and independent variables, quantitative research is an appropriate approach (Labaree, 2009; McCusker & Gunaydin, 2015). Additionally, the questionnaire includes an open-ended question which provides a more complete picture of the study and acquire greater insights in this research (Matveev, 2002; Osbaldeston, 2021).

### 3.4. Study Site

This research was carried out at the University of KwaZulu-Natal in Pietermaritzburg and Westville campus, situated in the province of KwaZulu-Natal, South Africa. Pietermaritzburg and Westville are two of the five campuses of the University of KwaZulu-Natal, namely Westville, Howard College, Edgewood, Nelson Mandela Medical School and Pietermaritzburg campus. Consists of the College of Agriculture, Engineering and Science, College of Law and Management Studies, College of Humanities, and College of Health Sciences. The study is limited to the students' (Undergraduates and postgraduate) population.

### 3.5. Target Population

In accordance with Explorable (2016), the target population generally means the sum of the people the researchers wants to generalise their findings to. The target population is taken from the study site which consists of the individuals for whom the survey is being conducted upon (Bhattacherjee, 2012). The study site is the University of KwaZulu-Natal, Pietermaritzburg and Westville campus. The target population is all 19 646 registered students from the University of KwaZulu-Natal, Pietermaritzburg campus and Westville campus. The target population figure was attained from the UKZN Institutional Intelligence Report (2022).

### 3.6. Pilot Study

The pilot research was carried out during a practical session, and 30 participants took part in the pilot. The pilot was used to check for omissions or discrepancies in the questionnaire. The results of the pilot test indicated that there were instances of non-response to certain questions, suggesting the need for revisions such as simplification of the question language or rephrasing, or that the overall length of the questionnaire may have been a contributing factor. Before sampling could begin, the omissions or discrepancies that were discovered were resolved. The findings of the pilot were not included in the final study.

### 3.7. Sampling Process

According to Latham (2007), sampling is a process where a small sample that represents a population is chosen for research. However, Frey et al. (2000) described the sample as a "subgroup" of a population. Trochim (2006) states that utilizing a sample of a population enables the researcher to generalise the outcome of the research to suit the whole population.

### 3.8. Study's Sample Size

According to UKZN Institutional Intelligence Report (2022), there are currently 19 646 registered students for the year 2022. The target population will therefore consist of 19 646 registered students. Based on Krejcie and Morgan (1970)'s sampling table, the sample size was 376 registered students.

### 3.9. Sampling Strategies

This research employed probability sampling as it reduces systematic and sampling bias. Probability sampling also ensures that the sample is representative of the target population by giving all the students in the sampling structure an equal chance to participate in the research (Bhardwaj, 2019). Therefore, this ensures that the research attains a higher reliability degree. This research utilised the **Stratified Sampling** (disproportional) method, and the sample was divided into four groups(strata), first years, second years, third years and postgraduates. Hence, 94 students from each group (strata) were selected. The research utilised a disproportional sampling method as 94 students from each year are not in proportion to their contribution to the total. The researcher gathered data in university lecture classrooms after classes had ended to ensure that all students at each year level had an equal opportunity to participate. The researcher employed simple

random sampling to select participants within the classroom. Moreover, the researcher utilised a random number generator to select participants within the classroom. Furthermore, all the participants of the study were from the College of Agriculture, Engineering and Science, College of Law and Management Studies and College of Humanities

### 3.10. Data Collection Methods

A questionnaire was utilised to gather information since this research used a quantitative approach methodology. A questionnaire is a tool utilised to extract information from students (Bhattacherjee, 2012). Moreover, questionnaires are generally utilised because they are inexpensive and efficient in obtaining information from a large sample and where interviews are impossible to conduct. Since this research has a large sample of 376 students, a questionnaire worked well as a data collection tool. The questionnaire includes both open-ended and closed-ended questions. Open-ended question help to collect extra data, which would not have been possible with closed-ended questions. In addition, the Likert scale type of questions were utilised. Data collection took 4 weeks to complete.

### 3.11. Data Quality Control

To guarantee the validity of the questionnaire, the researcher reused questionnaires from previous similar studies as shown in Table 3-1 and Appendix C. In addition, the questionnaires were assessed by a statistician to ensure that they were aligned with the research objectives. Vague questions were eliminated through a pilot test. In order to determine how reliable the information obtained from each part of the questionnaire is, Cronbach's alpha (Lee Cronbach, 1951) and factor analysis were performed.

Reliability refers to the consistency or stability of measurement, and one measure often used to assess reliability is Cronbach's alpha (Barbera et al., 2020; Cronbach, 1951; Sürücü & Maslakçi, 2020). This measure of internal consistency reliability ranges between 0 and 1, with a high score typically above 0.7 indicating that the items on a scale or questionnaire are highly correlated with one another, measuring the same construct consistently (Barbera et al., 2020; Cronbach, 1951; Sürücü & Maslakçi, 2020). Schrepp (2020) argues that a score above 0.4 indicates a high correlation.

Validity, on the other hand, pertains to the extent to which a study measures what it is intended to measure (Schrepp, 2020; Sürücü & Maslakçi, 2020). One method commonly used to establish construct validity is factor analysis. This statistical technique is used to

identify the underlying structure of a set of variables by identifying the common factors underlying the correlation among the variables.

Factor analysis is a widely used statistical technique that has been traditionally employed to aid in the establishment of construct validity. The primary aim of factor analysis is to identify the underlying structure of a set of variables by uncovering the common factors that underlie the correlation among them (Schrepp, 2020; Sürücü & Maslakçi, 2020).

In addition, it is essential to note that reliability and validity are not mutually exclusive and are often used together to establish the overall trustworthiness of the research (Schrepp, 2020; Sürücü & Maslakçi, 2020).

| PMT Constructs | Likert Questionnaire Items |
|---|---|
| Perceived Vulnerability | I could be a victim of a serious information security threat. (Burns et al., 2017; Ifinedo, 2012; Siponen et al., 2014) |
| | UKZN could be subjected to a serious information security threat. (Burns et al., 2017; Siponen et al., 2014) (Ifinedo, 2012) |
| | UKZN faces more and more serious information security threats lately. (Burns et al., 2017; Siponen et al., 2014) |
| Perceived Severity | An information security breach at UKZN will be a serious problem for me. (Ifinedo, 2012; Siponen et al., 2014) |
| | I will lose vital information if my login credentials are stolen. (Siponen et al., 2014) |
| | My privacy will be seriously violated if my login credentials are stolen. (Siponen et al., 2014) |
| | I will be in serious trouble if someone accesses the computer rooms using my student card. (Siponen et al., 2014) |
| | I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network. |
| Perceived Rewards | I would feel rewarded if a friend uses my student card to access the LAN. (Bakar et al., 2021; Burns et al., 2017; Posey et al., 2011; Sommestad et al., 2015) |
| | I would feel rewarded if a friend uses my LAN credentials to access the university network. (Bakar et al., 2021; Burns et al., 2017; Posey et al., 2011; Sommestad et al., 2015) |
| | I benefit from ***NOT*** complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. (Bakar et al., 2021; Burns et al., 2017; Sommestad et al., 2015) |

| | |
|---|---|
| Response Efficacy | I believe that ***NOT*** sharing my LAN login details prevents or reduces the chances of identity theft. (Ifinedo, 2012; Siponen et al., 2014) |
| | I believe that ***NOT*** sharing my student card helps to reduce security breaches. (Siponen et al., 2014) |
| | If I comply with information security policies, Information Systems security breaches will be scarce. (Burns et al., 2017; Ifinedo, 2012; Siponen et al., 2014; Sommestad et al., 2015) |
| Self-efficacy | I can comply with UKZN information security measures by myself. (Burns et al., 2017; Ifinedo, 2012; Siponen et al., 2014; Sommestad et al., 2015) |
| | I need assistance to comply with UKZN information security measures. (Burns et al., 2017; Siponen et al., 2014) |

***Table 3-1: Likert questionnaire items used for each construct***

### 3.12. Data Analysis

Correlation and regression analysis are statistical techniques that are frequently utilised to investigate the relationship between multiple variables. Correlation analysis aims to quantify the strength and direction of the relationship between two variables, typically done through measures such as the Spearman (non-parametric) or Pearson Correlation (parametric) coefficient, which ranges from -1 to 1. indicating a negative or positive correlation, respectively (Puniya & Singh). Regression analysis, on the other hand, aims to model the relationship between one or more independent variables and a dependent variable, by identifying the line (or equation) that best describes the relationship between the variables. Through this method, the effect of each independent variable on the dependent variable can be determined and predictions about the dependent variable can be made based on the values of the independent variables (Puniya & Singh)

A correlation analysis test was conducted between the Protection Motivation Theory constructs and students' compliance behaviour with the existing information security measures. Furthermore, a regression analysis was conducted to show a relationship between the construct (coping and threats appraisal) of protection motivation theory on student's compliance behaviour with the existing information security measures.

A positive correlation between the PMT constructs and students' compliance behaviour would indicate that students who perceive a high threat and coping appraisal are more likely to comply with information security measures, and vice versa for a negative correlation. Through regression analysis, the researcher would conduct regression analysis to test whether the PMT constructs could be used to predict students' compliance behaviour with information security measures. By doing this, the researcher could identify the variables which are the most predictive of compliance behaviour and focus on these to recommend new strategies to increase the students' compliance.

Data analysis is the process of organizing data to allow the extraction of significant information through the use of quantitative and/or qualitative analysis methods and thereafter arrive at a meaningful conclusion (Abulela & Harwell, 2020; Lemon & Hayes, 2020). This research utilised a quantitative, the information extracted from the open-ended question was used to strengthen, or add to the quantitative findings. The researcher used descriptive statistics (frequency analysis) to have a sense of the demographic distribution of the respondents according to their age, gender as well as other information pertaining to their education. A test of normality was performed to determine if the data were normally distributed or not, and this action was taken in order to determine which type of Correlation analysis to conduct between Spearman or Pearson Correlation. The Cronbach alpha coefficient was defined using the reliability tests for every segment and determining if the information is regularly distributed or skewed (Cronbach, 1951).

### 3.13. Handling Non-response Bias

As beneficial as a questionnaire-based study may appear, it is frequently susceptible to systematic bias, the non-response bias. This bias occurs when participants fail to complete the questionnaires and consequently affecting the study. The researcher overcame this by ensuring that the questionnaire asked questions that were simple and clear to improve the response rate. Furthermore, guaranteeing confidentiality to participants may aid in response rate improvement (Bhattacherjee, 2012). Therefore, prior to filling out the questionnaire, the participants were provided with an informed consent letter assuring participants of the study's confidentiality.

### 3.14. Ethical Consideration

Anonymity and confidentiality were maintained because sensitive information was not revealed, and participants' names were separated from their responses. For a period of

five years, the study data will be kept in the discipline of Information Systems and Technology in a secure location. After this time, data will be deposed. The researcher presented the research proposal in order to obtain ethical clearance from the University of KwaZulu- Natal's Ethics Committee, which was approved (Appendix A). According to Bhattacherjee (2012), ethical clearance is obtained to guarantee that the researcher does not modify the findings to suit the researcher's personal needs. This ensures that the research ethics of the university are followed during the course of this research. Before handing out questionnaires, a knowledgeable consent letter was handed out to prospective participants. The letter specified that participation is of their own free will, they are not forced to participate in the research, there is no financial reward for participating in the research, and they are allowed to withdraw from participation at any point. Students were given the assurance that declining to participate would have no negative consequences on their academics. Students were requested to sign the letter given to them if they agreed with its terms and conditions to use the information.

### 3.15. Concluding Remarks

This section discussed the methodology of this research and described the use of a descriptive design and utilised quantitative techniques to attain its goals. This chapter discussed the data collection method (questionnaires) and data analysis. Furthermore, this chapter addressed the handling of non-response bias by guaranteeing confidentiality and clear questions in the questionnaire. Finally, this chapter discussed how the study's ethics were adhered to. The following chapter analyses the data of the research and discusses the findings of the research.

# CHAPTER 4: DATA ANALYSIS AND FINDINGS

## 4.1. Introduction

This chapter presents the analysis of the responses attained from students. This chapter reveals the procedures taken to test the reliability and validity of the questions within the questionnaire and how the data was checked for any missing values. Test for normality and descriptive statistical analysis of the data is performed in this chapter. Furthermore, correlation, regression and thematic analysis are conducted in this chapter. This section reports on the findings based on the responses from participants, additional interpretation and discussion are provided in chapter 5

## 4.2 Handling missing data

Determining whether the data consists of any omitted value prior to performing any statistical analysis is crucial (Schafer & Olsen, 1998). Normally, missing values happen due to the failure of the respondents to answer certain questions within the questionnaire and when the respondents do not want to reveal confidential information. In addition, when the arrangement or structure of the research instrument is unfamiliar, the respondents tend to overlook a set of questions during data capturing (Field, 2013). For this research, missing values were found. This occurs when respondents fail to respond and overlook some questions. Subsequently, the researcher replaced missing values with the code “999” in SPSS, and it was clearly stated in the “missing data” field within the “variable view” in SPSS. The discovered missing values in this study are below 4% of the entire data set.

## 4.3. Reliability and Validity Tests

### 4.3.1. Reliability Analysis (Cronbach alpha test)

This section determines the coherence and dependability of the research instrument (questionnaire). The Cronbach’s Alpha test was utilised to assess the internal coherence of the questions and ensure the dependability of the questionnaire. Igbaria and Iivari (1995) proposed that the average variance should be greater or equal to 0.5 for a questionnaire to pass the consistency and reliability test. At the same time, Leech et al. (2005) argued that the average variance should be equal to or above 0.7. When Cronbach's Alpha is between 0.8 and 0.9, the researcher interpreted the data as with very high internal consistency. When Cronbach's Alpha was equal to or above 0.7, the researcher interpreted data with high internal consistency. When Cronbach's Alpha was less than 0.5, the researcher considered the data as with no internal consistency. The reliability test

excluded the demographic questions and only consisted of the Likert scale questions. Table 4-1 below presents the reliability statistics for the questions in the overall questionnaire.

| Constructs within the Questionnaire | Number of Items | Cronbach's Alpha (α) | Interpretation |
|---|---|---|---|
| Physical access to computer rooms | 3 | .389 | Close to adequate internal consistency |
| Access to the University network | 9 | .360 | Close to adequate internal consistency |
| Awareness of UKZN information systems policies | 4 | .777 | High internal consistency |
| Perceived Vulnerability | 3 | .700 | High internal consistency |
| Perceived Severity | 5 | .720 | High internal consistency |
| Perceived rewards | 3 | .728 | High internal consistency |
| Response Efficacy | 3 | .823 | Very high internal consistency |
| Self-efficacy | 3 | .125 | low internal consistency |
| Response Cost | 3 | .837 | Very high internal consistency |
| Challenges to information security compliance | 7 | .807 | Very high internal consistency |
| **Overall** | **43** | **.704** | **High internal consistency** |

***Table 4-1: Reliability Statistics***

Table 4-1 above shows that there is internal consistency with the overall questions from the questionnaire above (i.e. $\alpha > 0.7$). Overall, the questionnaire has a high internal consistency ($\alpha = 0.704$). Subsequently, the questionnaire can be considered to be consistent and reliable.

### 4.3.2. Construct Validity Test (Factor Analysis)

Factor analysis is a type of dimension reduction and summarization procedure. (Dheri et al., 2019). Principal components analysis (PCA) is an extraction method within the Factor analysis process (Mendonça et al., 2021). Mendonça et al. (2021) and Tianxiao et al. (2009) state that PCA is a variable-reduction technique that seeks to reduce a bigger sets of variables to a small sets of "artificial" variables, known as "principal components". These composite components can represent information from the original variable and they are pairwise independent, thus, simplifying the original variables (Laerd, 2022; Tianxiao et al., 2009).

Confirmatory factor analysis (CFA) is a statistical technique that is commonly used in survey research to validate questionnaire items. CFA is used to test the hypothesis that a set of questionnaire items is measuring a particular construct or latent variable and to assess the overall fit of the model to the data. The researcher conducted a Confirmatory factor analysis to validate the questionnaire items to the dependent and independent variables as shown in Figure 4-1 below. Moreover, CFA provides evidence for construct validity by demonstrating that the observed variables are reliable indicators of the latent constructs they are intended to measure.

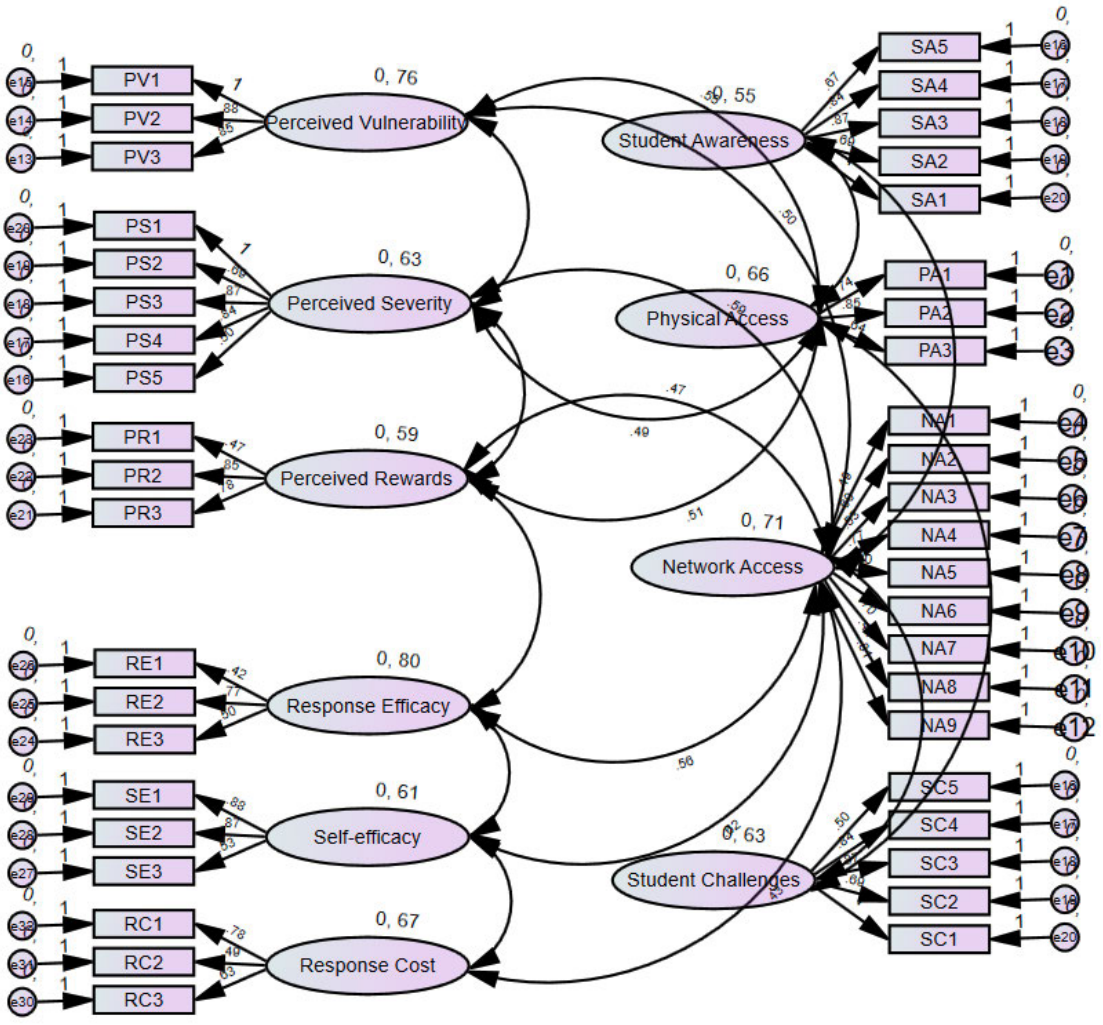



***Figure 4-1: Confirmatory Factor Analysis (CFA) – Dependent and Independent Variables of Respondents***

Factor analysis has been widely used in the field of information security to create indices. The use of factor analysis in this context is supported by several recent studies demonstrating its effectiveness. Chandra et al. (2022) and Tu and Yuan (2014) conducted studies that applied factor analysis to a dataset of information security-related variables and identified a set of factors that were used to construct an information security index.

The studies found that the use of factor analysis was a useful approach for creating an information security index. Moreover, these studies, and others like them (Knekta et al., 2019), provide recent academic motivation for the use of factor analysis in creating an information security index value. They demonstrate that this technique can effectively extract the data sets and that it can be used to create indices that are easy to interpret, specifically in the context of information security.

Kaiser-Meyer-Olkin (KMO) and Bartlett's test measures whether it is appropriate to conduct the FA test. Kaiser-Meyer-Olkin Measure of Sampling Adequacy varies between 0 and 1, and values closer to 1 are ideal. The proposed rule-of-thumb is KMO >= 0.5 (Dheri et al., 2019). Bartlett's Test of Sphericity tests whether the data is suitable for data reduction, further indicating that FA can be carried out, Sig = 000 (Laerd, 2022).

Factor analysis is performed on Student Compliance constructs in order to provide important insights into the underlying factors that influence student compliance in higher education institutions. By analysing the factors that contribute to student compliance, the researcher can identify the key drivers of behaviour, understand the relationships between these factors and PMT constructs. Factor Analysis is relevant to the dependent variable that is represented in Section B of the questionnaire where there are 3 sub-sections that equate to 3 internal constructs for the dependent variable. Furthermore, Factor Analysis was performed on the construct named Student's Compliance with Physical Access to Computer Rooms construct on the questionnaire, and it revealed that the Physical Access to Computer Rooms consists of one component/factor. Moreover, KMO and Bartlett's test confirmed that it is appropriate to carry out the FA test as KMO >.5 (KMO = .514) and Bartlett's Test of Sphericity sig = .000 as shown in Table 4-2 and Table 4-3 respectively below.

| KMO and Bartlett's Test | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .581 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 332.905 |
| | df | 36 |
| | Sig. | .000 |

***Table 4-2: KMO and Bartlett's test - Physical Access to Computer Rooms***

| Component Matrix[a] | |
|---|---|
| | Component |

| | 1 |
|---|---|
| 7.2. I sometimes ask students to grant me access to computer facilities (LANs) | .864 |
| 7.3. I sometimes let students access the LANs using my student card. | .849 |
| 7.1. I always use my student card to access computer facilities (LANs) | -.313 |

***Table 4-3: Factor Analysis Test - Physical access to Computer Rooms***

KMO and Bartlett's test confirmed that the data is suitable to conduct factor analysis test as KMO >.5 (KMO = .581) and Bartlett's Test of Sphericity sig = .000 as shown in Table 4-4 below. Factor analysis was performed on Student Compliance with Access to the University Network. Factor analysis revealed that Access to the University Network consists of three components/factors as shown in Table 4-5 below. Factor 1 includes questions 8.1 "I always use my personal login details and password to login into UKZN network", 8.2 ("I sometimes use someone else login details (username and password) to access the university network"), 8.3 ("I sometimes allow other people to use my login details (username and password) to access the university network"), and 8.6. ("The password that I use to access the UKZN network is unknown to anyone else"). Factor 2 includes questions 8.4 ("I always change my password (to access the University network) at least once in 3 months"), 8.7 (I provide my UKZN login details when requested via email), 8.8 (I take information security precautionary measures as advised through the UKZN email alerts) and 8.9 (I have been a victim of phishing scams (email scams) while using the UKZN network). Factor 3 includes question 8.5 ("I always use a password with a combination of letters, numbers and symbols (@, #, $, %, etc.) to access the University network as recommended by the UKZN ICS department").

| KMO and Bartlett's Test | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .581 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 332.905 |
| | df | 36 |
| | Sig. | .000 |

***Table 4-4: KMO and Bartlett's test - Access to the University Network***

| Component Matrix[a] | | | |
|---|---|---|---|
| | Component | | |
| | 1 | 2 | 3 |
| 8.3. I sometimes allow other people to use my login details (username and password) to access the university network | -.770 | | |
| 8.2. I sometimes use someone else login details (username and password) to access the university network | -.746 | | .333 |
| 8.6. The password that I use to access the UKZN network is unknown to anyone else. | .476 | | .419 |
| 8.1. I always use my personal login details and password to login into UKZN network | .464 | | -.322 |
| 8.4. I always change my password (to access the University network) at least once in 3 months | | .685 | |
| 8.7. I provide my UKZN login details when requested via email | | .610 | |
| 8.9. I have been a victim of phishing scams (email scams) while using the UKZN network | | .562 | -.493 |
| 8.8. I take information security precautionary measures (e.g. frequently changing password, not sharing login details, not click on unknown email links etc.) as advised through the UKZN email alerts. | .454 | .484 | |
| 8.5.I always use a password with a combination of letters, numbers and symbols (@, #, $, %, etc.) to access the University network as recommended by the UKZN ICS department. | | | .625 |
| Extraction Method: Principal Component Analysis. | | | |
| a. 3 components extracted. | | | |

***Table 4-5: Factor Analysis Test - Access to the University Network***

KMO and Bartlett's test confirmed that the data is appropriate to conduct factor analysis test as KMO >.5 (KMO = .698) and Bartlett's Test of Sphericity sig = .000 as shown in Table 4-6 below. Factor analysis was performed on the awareness of UKZN information systems policies, factor analysis revealed that awareness of UKZN information systems policies consists of 1 factor as shown in and Table 4-7 below.

| KMO and Bartlett's Test | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .698 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 582.229 |
| | df | 6 |
| | Sig. | .000 |

***Table 4-6: KMO and Bartlett's test - awareness of UKZN Information Systems Policies***

| Component Matrix[a] | |
|---|---|
| | Component |
| | 1 |
| 9.2. I am aware of UKZN policies regarding access to the UKZN network | .914 |
| 9.1. I am aware of UKZN policies regarding physical access to computer rooms/ LAN | .877 |
| 9.3. I am aware of UKZN policies regarding choosing a strong password | .731 |
| 9.4. I do check the ICS website regularly to acquaint myself with new information security alerts | .559 |
| Extraction Method: Principal Component Analysis. | |
| a. 1 components extracted. | |

***Table 4-7: Factor Analysis Test - Awareness of UKZN Information Systems Policies***

An index was generated for each one of these factors through principal components analysis. These indexes were then correlated with the Protection Motivation Theory's constructs in the following sections from 4.6.2 – 4.6.5 below.

### 4.4 Test for Normality

To determine the type of analysis to perform on the obtained data, it is important to establish whether the data is normally distributed or not. A Kolmogorov-Smirnov and Shapiro-Wilk normality tests were performed to establish the distribution of the data. If the data is normally distributed, a parametric correlation (Pearson Correlation) would be an appropriate type of analysis to conduct. However, if the data is not normally distributed, then a non-parametric correlation (Spearman Correlation) would be an appropriate type of analysis. Laerd (2013) and Pallant (2013) state that when a Kolmogorov-Smirnov and Shapiro-Wilk test is conducted, and the significance value is less than 0.05 (sig < 0.05), then that data set can be deemed to be not normally distributed. However, when a test returns a significance value greater than 0.05 (sig > 0.05), it is normally distributed. The significance value of this study is less than 0.05 (sig < 0.05) as shown in Table 4-6. Therefore, a non-parametric test (Spearman Correlation) is the appropriate test for this study.

| Tests of Normality | | | | | | |
|---|---|---|---|---|---|---|
| | Kolmogorov-Smirnova | | | Shapiro-Wilk | | |
| | Statistic | df | Sig. | Statistic | df | Sig. |
| Physical access to computer rooms | .200 | 269 | .000 | .931 | 269 | .000 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Access to the University network | .035 | 269 | .000 | .995 | 269 | .000 |
| Awareness of UKZN information systems policies | .116 | 269 | .000 | .934 | 269 | .000 |
| Perceived Vulnerability | .088 | 269 | .000 | .968 | 269 | .000 |
| Perceived Severity | .108 | 269 | .000 | .911 | 269 | .000 |
| Perceived Rewards | .217 | 269 | .000 | .783 | 269 | .000 |
| Response Efficacy | .184 | 269 | .000 | .926 | 269 | .000 |
| Self-Efficacy | .088 | 269 | .000 | .980 | 269 | .001 |
| Response Cost | .139 | 269 | .000 | .960 | 269 | .000 |
| Challenges to information security compliance | .051 | 269 | .042 | .992 | 269 | .032 |

***Table 4-6: Test of Normality***

## 4.5 Demographics

### 4.5.1. Age of Respondents

This study was conducted amongst 376 participants, and the demographics of the respondents indicate that most participants were between the ages of 18 and 24 (N = 341, 90.7%), followed by participants between the ages of 25 – 30 (N = 24, 6.4%), 31 and above (N = 7, 1.9%), and least respondents were less than 18 (N = 4, 1.1%) of age as shown in Figure 4-2 and Appendix F.

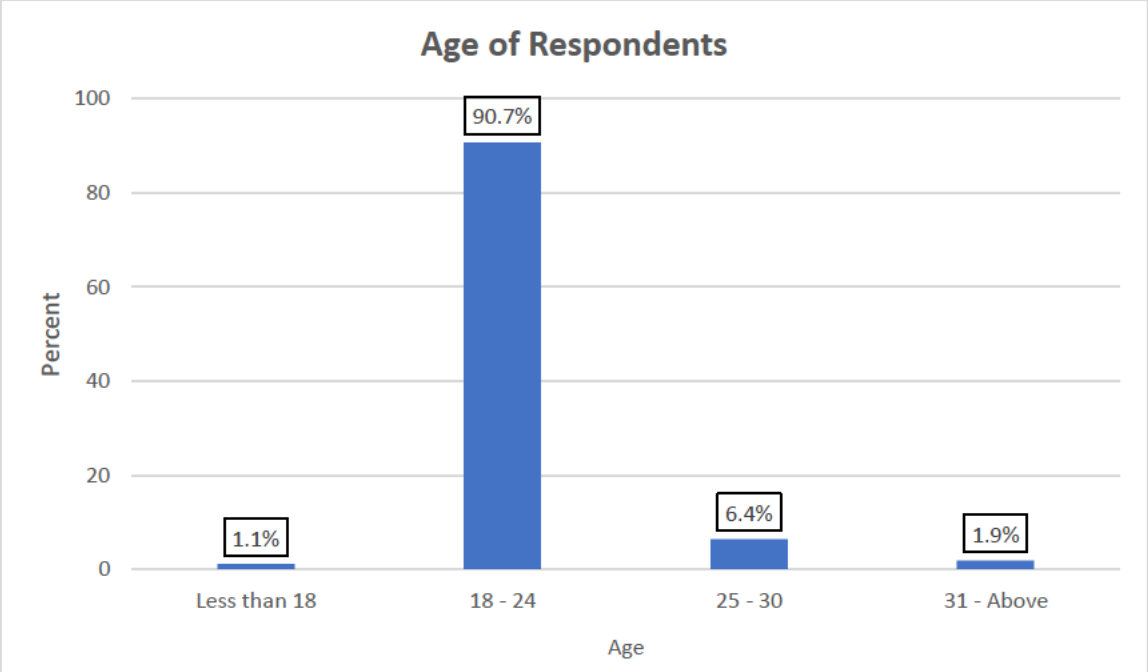


*Figure 4-2: Age of Respondents*

### 4.5.2. Gender of the Respondents

The study had 376 respondents, Figure 4-3 and Appendix F show that there were more male respondents (N = 207, 55.1%) than female respondents (N = 169, 44.9%). Therefore, male students had more representation in the study than female students.

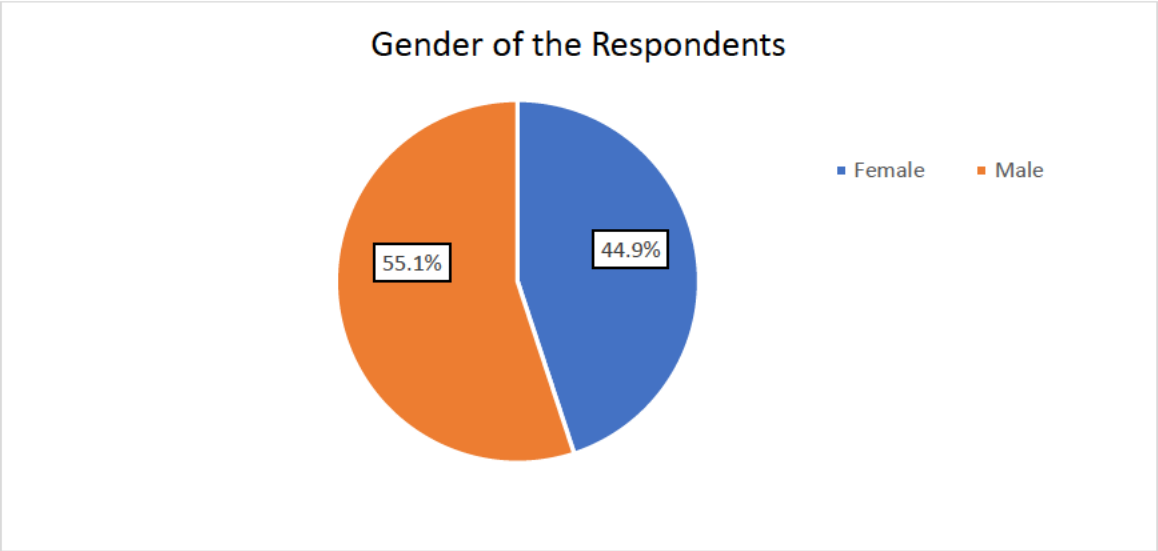



*Figure 4-3: Gender of Respondents*

### 4.5.3 Ethnicity of the Respondents

The research was carried out in South Africa, a nation consisting of diverse ethnic groupings. As shown in Figure 4-4 below and Appendix F, the majority of the respondents were African (N = 301, 80.1%), followed by Indian (N = 59, 15.7%), thereafter, Coloured (N = 8, 2.1%), then White (N = 6, 1.6%) with the lowest representation ethnic group in this study.

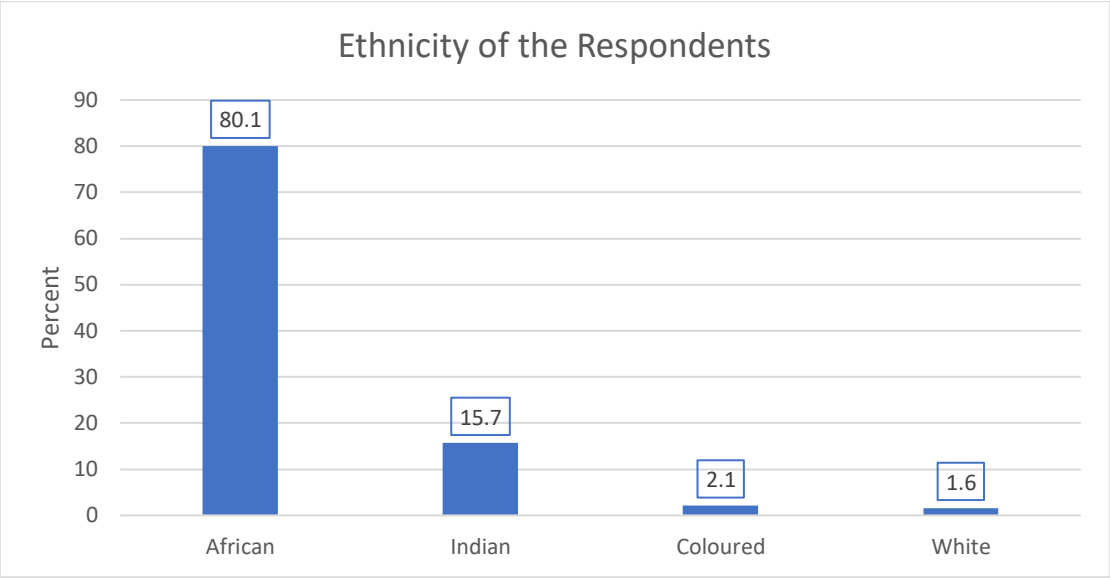



***Figure 4-4: Ethnicity of the Respondents***

### 4.5.4 Level of Study of the Respondent

The respondents of this research were students their First year (N = 88, 23.4%), Second year (N = 91, 24.2%), Third year (N = 136, 36.2%), Honours (N = 48 12.8%), Masters (N = 8, 2.1%), and PhD (N = 5, 1.3%) academic level. This is supported by Figure 4-5 below and Appendix F.

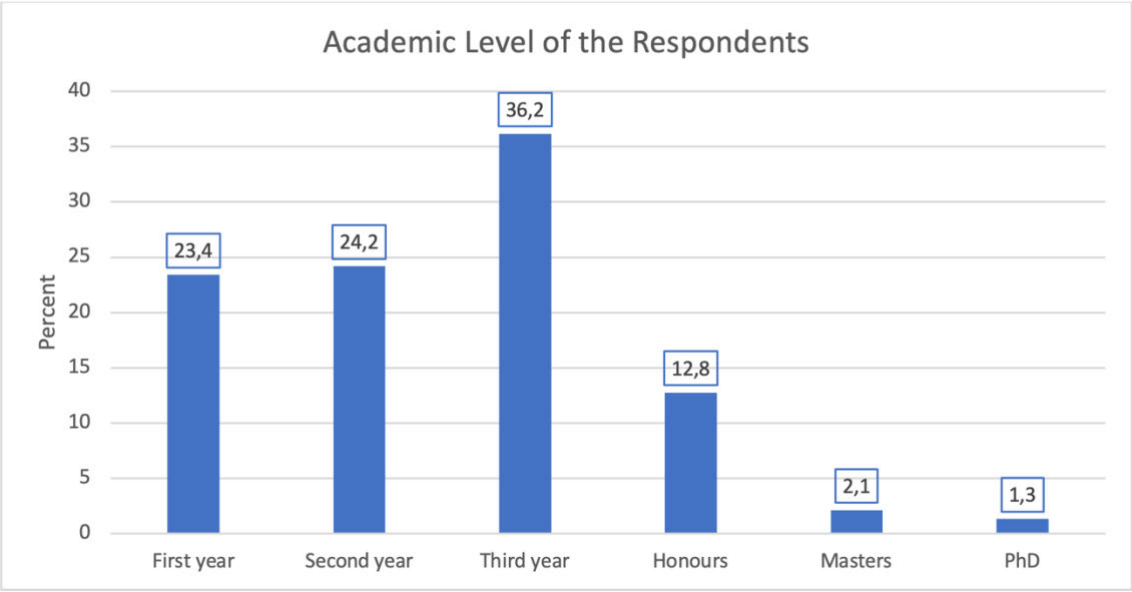



***Figure 4-5: Level of Study of the Respondent***

### 4.5.5 Campus of the Respondents

The respondents of this study were students in Pietermaritzburg (N = 196, 52.1%) and Westville (N = 180, 47.9%) campuses, as shown in Figure 4-6 and Appendix F below.

The respondents represent 1.9% of the target population (19 646) from the University of KwaZulu-Natal, Pietermaritzburg campus and Westville campus.

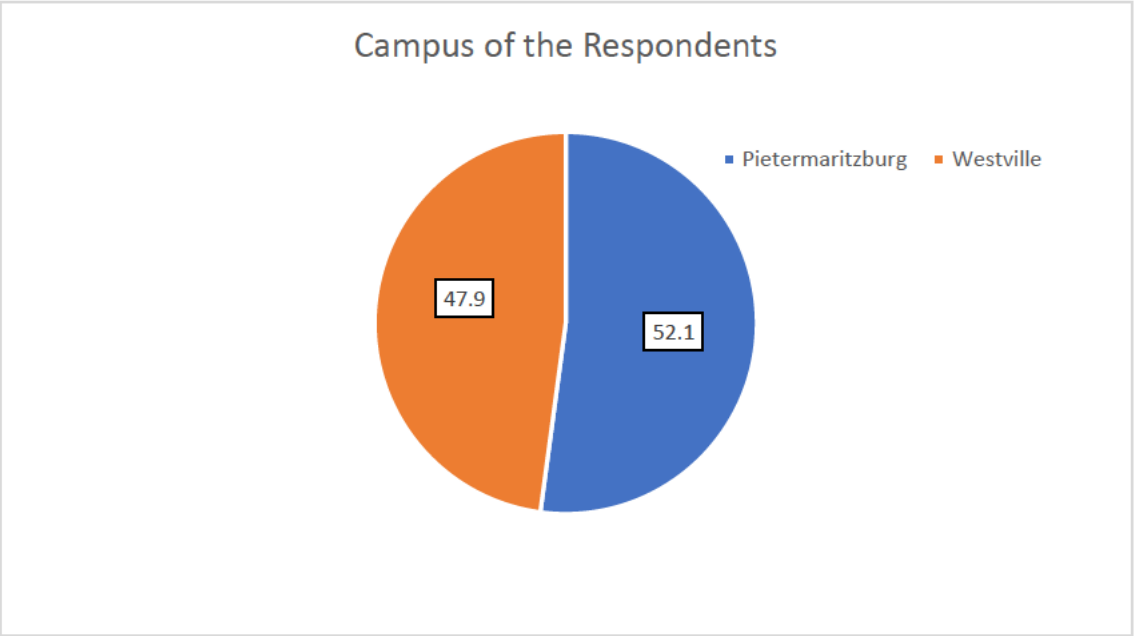



***Figure 4-6: Campus of the Respondents***

### 4.6. Answering the Research Questions

The participants answered questions based on the Protection Motivation Theory constructs from this research's conceptual model. The constructs include Perceived Vulnerability, Perceived Severity, Perceived Rewards, Response Efficacy, Self-Efficacy, Response Cost and Student Compliance. The following are the responses to all the constructs questions using a Likert scale ranging from "Strongly Agree" (5) to "Strongly Disagree" (1). This is also displayed in Appendix G.

Correlation analysis is employed to determine a linear relationship between two variables. The linear relationship strength is calculated using the correlation coefficient unit (Nickolas, 2021). Furthermore, if the correlation coefficient is larger than zero that implies a positive association, whilst a correlation coefficient unit below zero suggests a negative association. Subsequently, a Linear Regression test is performed to produce a "p" value frequently referred to as Asymptotic (Asymp.) Significance (Sig.). In a case where the "p" score that is produced from a regression analysis test is higher than 0.05, that will suggest no statistical significance among the variables; however, in a case where the "p" score calculated from a regression analysis test is below 0.05, that would suggests that the factors are significantly correlated (Rengganis & Katmini, 2021).

### 4.6.1. Research Question 1: How Compliant are Students with the Existing Information Security Measures Currently in Place within the University?

The participants answered questions based on questionnaire subsections: Physical Access to Computer Rooms, Access to the University Network and Awareness of UKZN Information Systems Policies. The following are the responses to all the questions using a Likert scale ranging from "Strongly Agree" (5) to "Strongly Disagree" (1). This is also displayed in Appendix G.

#### 4.6.1.1. Descriptive Analysis of the Student's Compliance with Physical Access to Computer Rooms

Most students agree (a consolidated percentage of students that agree and strongly agree) that they always utilise their student identification cards to enter the computer facilities (N=376, 93.6%). In addition, most students agree that they sometimes ask other students to give them access to the computer facilities (N=375, 51.7%), consequently, most students sometimes let other students access the computer rooms using their cards (N=376, 60.3%). This is corroborated by Table 4-7 below and Appendix G which shows the mode (i.e. the most frequently chosen answer) for question 7.1 (I always use my student card to access computer facilities (LANs)) is 5 indicating that most students strongly agreed that they always use their student cards to access computer facilities. Moreover, question 7.2 (I sometimes ask students to grant me access to computer facilities (LANs)) has a mode is 4 indicating that students agree that they sometimes ask students to grant them access to computer facilities. In addition, question 7.3 (I sometimes let students access the LANs using my student card) has a mode of 4 indicating that students agree that sometimes they let other students access the LAN using their student cards. As per the University rules, students are not permitted to let others utilise their student cards to access the LANs (Information & Communication Services, 2022). Hence, from these responses students are not abiding by this rule.

| Statistics | | | | |
|---|---|---|---|---|
| | | 7.1. I always use my student card to access computer facilities (LANs) | 7.2. I sometimes ask students to grant me access to computer facilities (LANs) | 7.3. I sometimes let students access the LANs using my student card. |
| N | Valid | 376 | 375 | 376 |
| | Missing | 0 | 1 | 0 |
| Mean | | 4.60 | 3.25 | 3.49 |
| Median | | 5.00 | 4.00 | 4.00 |
| Mode | | 5 | 4 | 4 |
| Std. Deviation | | .727 | 1.312 | 1.226 |

***Table 4-7: Frequency of Student Compliance with Physical Access to Computer Rooms***

#### 4.6.1.2. Descriptive Analysis of the Student's Compliance with Access to the University Network

The majority of students agree (a consolidated percentage of students that agree and strongly agree N=376, 98.2%) that they utilise their own login credentials to access the UKZN network at all times. Furthermore, most students disagree that they sometimes use someone else's login credentials to access the university network (N=3767, 81.7%). Moreover, most students disagree that they sometimes allow other people to use their login credentials to access the university network (N=376, 75.8%). Furthermore, the majority of the students disagree that they change their password at least once every three months (N=376, 69.9%). Moreover, the majority of the students agree that they always utilise a strong password to login into the university network as recommended by the UKZN ICS department (N=376, 84.1%). Furthermore, most students agree that no one else knows the password they utilise to access the UKZN network (N=376, 77.4%). Moreover, most students disagree that they provide their UKZN login details when requested via email (N=376, 49.5%). Furthermore, the majority of the students agree that they take information security precautionary measures as advised through the UKZN email alerts (N=376, 58.8%). Additionally, most students disagree that they have been a victim of phishing scams (email scams) while using the UKZN network (N=376, 71,6%). This is corroborated by Table 4-8 below and Appendix E that shows that the mode (i.e. the most frequently chosen answer) for question 8.1 ("I always use my personal login details and password to login into the UKZN network") is 5 indicates that most students strongly agreed that they utilise their own login credentials to access the UKZN network at all times. Furthermore, question 8.2 ("I sometimes use someone else login details

(username and password) to access the university network") which has a mode is 1 indicating that students strongly disagree that they sometimes use someone else login credentials to access the university network. Moreover, question 8.3 ("I sometimes allow other people to use login details (username and password) to access the university network") correspondingly has a mode of 1, depicting that students strongly disagree that they sometimes allow other people to use their login credentials to access the university network. In addition, question 8.4 ("I always change my password (to access the University network) at least once in 3 months") has a mode of 2 indicating that students disagree that they change their password at least once every three months. Furthermore, question 8.5 ("I always use a strong password to access the University network as recommended by the UKZN ICS department") with a mode of 5 indicates that students strongly agree that they always utilise a strong password to login into the university network as recommended by the UKZN ICS department. Moreover, question 8.6 ("The password that I use to access the UKZN network is unknown to anyone else") has a mode of 5 indicating that students strongly agree that no one else knows the password they use to get into the UKZN network. Furthermore, question 8.7 ("The password that I use to access the UKZN network is unknown to anyone else") has a mode of 1 revealing that students strongly disagree that they provide their UKZN login details when requested via email. Additionally, question 8.8 (I take information security precautionary measures as advised through the UKZN email alerts) has a mode of 5 displaying that most students strongly agree that they take information security precautionary measures as advised through the UKZN email alerts. Furthermore, question 8.9 (I have been a victim of phishing scams (email scams) while using the UKZN network) with a mode of 1 indicating that students strongly disagree that they have been a victim of phishing scams (email scams) while using the UKZN network. As per university rules, students are required to change their password at least once every three 3 months. Therefore, from these responses students are not abiding by the information security policy.

| Statistics | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 8.1. I always use my personal login details and password to login into UKZN network | 8.2. I sometimes use someone else login details (username and password) to access the university network | 8.3. I sometimes allow other people to use my login details (username and password) to access the university network | 8.4. I always change my password (to access the University network) at least once in 3 months | 8.5.I always use a password with combination of combination of letters, numbers and symbols (@, #, $, %, etc.) to access the University network as recommended by the UKZN ICS department. | 8.6. The password that I use to access the UKZN network is unknown to anyone else. | 8.7. I provide my UKZN login details when requested via email | 8.8. I take information security precautionary measures (e.g. frequently changing password, not sharing login details, not click on unknown email links etc.) as advised through the UKZN email alerts. | 8.9. I have been a victim of phishing scams (email scams) while using the UKZN network |
| N | Valid | 376 | 376 | 376 | 376 | 376 | 376 | 376 | 375 | 373 |
| | Missing | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 3 |
| Mean | | 4.85 | 1.82 | 2.00 | 2.13 | 4.24 | 4.07 | 2.84 | 3.63 | 2.10 |
| Median | | 5.00 | 1.00 | 2.00 | 2.00 | 5.00 | 5.00 | 3.00 | 4.00 | 2.00 |
| Mode | | 5 | 1 | 1 | 1 | 5 | 5 | 1 | 5 | 1 |
| Std. Deviation | | .463 | 1.102 | 1.178 | 1.135 | 1.055 | 1.226 | 1.662 | 1.220 | 1.253 |

***Table 4-8: Frequency of Student's Compliance with Access to the University Network***

#### 4.6.1.3. Descriptive Analysis of the Awareness of UKZN Information Systems Policies

Most students agree (a consolidated percentage of students that agree and strongly agree- N=376, 72%) that they are aware of UKZN policies regarding physical access to computer rooms/ LAN. Furthermore, most students agree that they are aware of UKZN policies regarding access to the UKZN network (N=376, 70.4%). Moreover, most students agree that they are aware of UKZN policies regarding choosing a strong password (N=293, 84.3%). In addition, more than half of the students disagree that they do check the ICS website regularly to acquaint themselves with new information security alerts (N=376, 57. 4%). This is represented by Table 4-9 below and Appendix E that shows the mode (i.e. the most frequently chosen answer) for question 9.1 (I am aware of UKZN policies regarding physical access to computer rooms/ LAN) is 4 indicating that

most students agreed that they are aware of UKZN policies regarding physical access to computer rooms/ LAN. Similarly, question 9.2 (I am aware of UKZN policies regarding access to the UKZN network) has a mode of 4 indicating that students agree that they are aware of UKZN policies regarding access to the UKZN network. Moreover, question 9.3 (I am aware of UKZN policies regarding choosing a strong password) has a mode of 4 indicating that students agree that they are aware of UKZN policies regarding choosing a strong password. However, question 9.4 (I do check the ICS website regularly to acquaint myself with new information security alerts) has a mode of 3 indicating that students do not agree or disagree that they do check the ICS website regularly to acquaint themselves with new information security alerts. As per the University rules, students are encouraged to check the ICS website regularly to acquaint themselves with new information security alerts and policies (Information & Communication Services, 2022). Hence, from these responses students are not abiding by this rule and students are not aware of the latest measures put in place by the university due to not regularly visiting the university ICS website.

| Statistics | | | | | |
|---|---|---|---|---|---|
| | | 9.1. I am aware of UKZN policies regarding physical access to computer rooms/ LAN | 9.2. I am aware of UKZN policies regarding access to the UKZN network | 9.3. I am aware of UKZN policies regarding choosing a strong password | 9.4. I do check the ICS website regularly to acquaint myself with new information security alerts |
| N | Valid | 376 | 376 | 375 | 376 |
| | Missing | 0 | 0 | 1 | 0 |
| Mean | | 3.84 | 3.80 | 4.12 | 2.60 |
| Median | | 4.00 | 4.00 | 4.00 | 3.00 |
| Mode | | 4 | 4 | 4 | 3 |
| Std. Deviation | | 1.031 | .993 | .802 | 1.150 |

***Table 4-9: Frequency of the Awareness of UKZN Information Systems Policies***

#### 4.6.1.4. Reasons for not Complying with Information Security Measures

The students were asked in an open-ended question to specify other factors preventing them from complying with UKZN information security measures in place. Furthermore, thematic analysis was performed on the student's responses to the open-ended question as shown in Figure 4-7. Most students (59%) who answered the question stated insufficient knowledge and comprehension of data security. Followed by students (14%) stating that they do not have enough time to educate themselves on data security.

Furthermore, another group of students (10%) is willing to learn but indicated that they are lazy to read these information security policies and security measures. Similarly, another group of students (10%) stated that the existence of the student card system causes them not to comply because they forget their student cards and need someone to give them access and vice versa. In addition, the last group of students (7%) stated that they lack attention to the email threats from the UKZN's Information & Communication Services (2022) department.

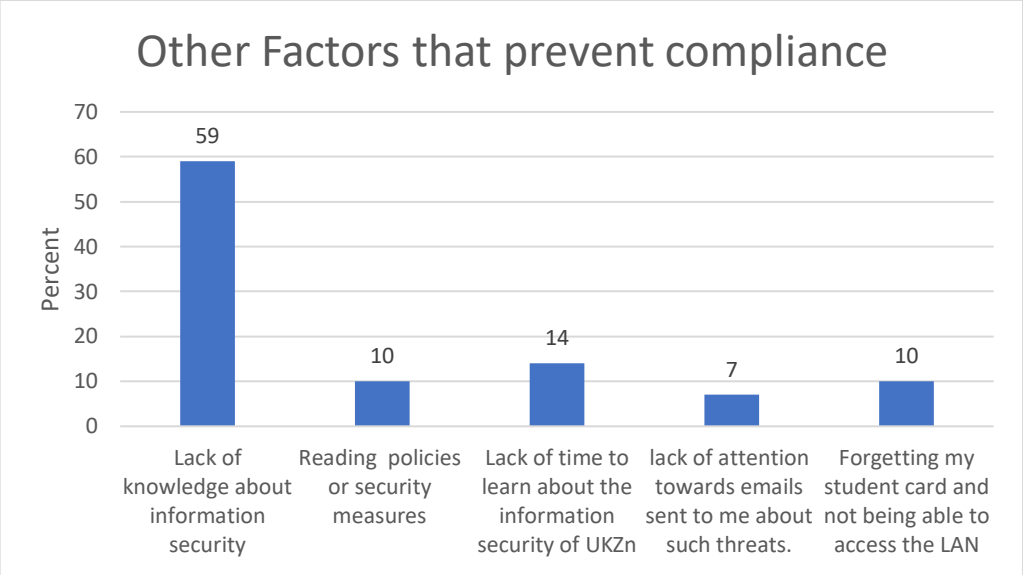



***Figure 4-7: Thematic Analysis of Other Factors that Prevent Compliance***

### 4.6.2. Research Question 2: What are the effects of Threat Appraisal on Students' Compliance with the Information Security Measures within the University?

The participants answered questions based on the Protection Motivation Theory construct (Threat Appraisal) from this research's conceptual model. The Threat Appraisal construct includes Perceived Vulnerability, Perceived Severity and Perceived Rewards. The following are the responses to all the questions using a Likert scale ranging from "Strongly Agree" (5) to "Strongly Disagree" (1). This is also displayed in Appendix G.

#### 4.6.2.1. Influence of Perceived Vulnerability on Students' Compliance with Information Security Measures in Place

**a) Descriptive Analysis of the Perceived Vulnerability Responses**

Most students agree (a consolidated percentage of students that agree and strongly agree) that they can be victims of a severe data security threat (N=375, 43.1%). Furthermore, the

majority of the students agree that UKZN can face a severe data security threat (N=376, 40.2%). Moreover, most students do not agree or disagree that UKZN faces a growing number of serious data security threats (N=376, 50.3%). This is corroborated by Table 4-11 below and Appendix E, which displays the mode (i.e. the most frequently chosen answer) for question 10.1 ("I could be a victim of a serious information security threat") to be 4 indicating that most students agree that they can be victims of a severe data security threat. However, question 10.2 ("UKZN could be subjected to a serious information security threat") has a mode of 3, indicating that most students do not agree or disagree that UKZN can be susceptible to a severe data security threat. Similarly, question 10.3 ("More and more serious information security threats are being faced by UKZN") has a mode of 3, indicating that most students agree nor disagree that UKZN faces a growing number of serious data security threats.

| Statistics | | | | |
|---|---|---|---|---|
| | | 10.1 I could be a victim of a serious information security threat | 10.2. UKZN could be subjected to a serious information security threat | 10.3. UKZN faces more and more serious information security threats lately. |
| N | Valid | 375 | 375 | 375 |
| | Missing | 1 | 1 | 1 |
| Mean | | 3.19 | 3.39 | 3.22 |
| Median | | 3.00 | 3.00 | 3.00 |
| Mode | | 4 | 3 | 3 |
| Std. Deviation | | 1.073 | .906 | .896 |

***Table 4-11: Frequency of Perceived Vulnerability***

### b) Correlation between Perceived Vulnerability and Physical Access to Computer Rooms

A Spearman correlation was performed between the independent construct named Perceived Vulnerability and the 1st construct from the dependent variable named Student Compliance; the 1st construct in the dependent variable is named Physical Access to Computer Rooms which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 3 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Vulnerability and the single index value generated for F1. The correlation reveals that there is a significant and positive correlation between F1 and students' perceptions that they can be victims of a severe data security threat (rho=0.219, p=0.000, N=374). Furthermore, the correlation

also reveals that there is a significant and positive correlation between F1 and students' perceptions that UKZN can be susceptible to severe data security threat (rho=0.158, p=0.002, N=374) as shown in Table 4-12 below. Subsequently, linear regression analysis was performed.

| Correlation | | | Q7 Physical access to computer rooms factor |
|---|---|---|---|
| Spearman's rho | Q7 Physical access to computer rooms | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 375 |
| | 10.1 I could be a victim of a serious information security threat | Correlation Coefficient | .219** |
| | | Sig. (2-tailed) | .000 |
| | | N | 374 |
| | 10.2. UKZN could be subjected to a serious information security threat | Correlation Coefficient | .158** |
| | | Sig. (2-tailed) | .002 |
| | | N | 374 |
| | 10.3. UKZN faces more and more serious information security threats lately. | Correlation Coefficient | .100 |
| | | Sig. (2-tailed) | .054 |
| | | N | 374 |
| **. Correlation is significant at the 0.01 level (2-tailed) | | | |

***Table 4-12: Correlation of Perceived Vulnerability vs Physical Access to Computer Rooms***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effects of the variables on compliance with measures put in place for physical access to computer rooms. As depicted in Table 4-13 below, the regression model significantly predicts the dependent variable outcome (p = 0.014). Student Compliance with Physical Access to Computer Rooms is represented by one regression model. The regression equation that represents the regression model is as follows: F1 = Constant + Regression Coefficient = -0.893+ 0.143 * X (where X represents, "I could be a victim of a serious information security threat").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.833 | .229 | | -3.635 | .000 |
| | 10.1 I could be a victim of a serious information security threat | .143 | .058 | .154 | 2.473 | .014 |
| | 10.2. UKZN could be subjected to a serious information security threat | .027 | .078 | .024 | .346 | .729 |
| | 10.3. UKZN faces more and more serious information security threats lately. | .088 | .066 | .080 | 1.334 | .183 |
| a. Dependent Variable: Q7 Physical access to computer rooms | | | | | | |

***Table 4-13: Regression of Perceived Vulnerability vs Physical Access to Computer Rooms***

### c) Correlation between Perceived Vulnerability and Access to the University Network

A Spearman correlation was performed between the independent construct named Perceived Vulnerability and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Vulnerability and the single index value generated for F1. The correlation reveals that there is no significant correlation between F1 and the Perceived Vulnerability construct, this is depicted in Table 4-14 below. Subsequently, a linear regression analysis was not conducted to assess the effect of the two variables.

| Correlation | | | Q8 Access to the University network f1 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f1 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 10.1 I could be a victim of a serious information security threat | Correlation Coefficient | .086 |
| | | Sig. (2-tailed) | .097 |
| | | N | 371 |
| | 10.2. UKZN could be subjected to a serious information security threat | Correlation Coefficient | -.007 |
| | | Sig. (2-tailed) | .898 |
| | | N | 371 |
| | 10.3. UKZN faces more and more serious information security threats lately. | Correlation Coefficient | .063 |
| | | Sig. (2-tailed) | .224 |
| | | N | 371 |

***Table 4-14: Correlation of Perceived Vulnerability vs Access to the University Network Factor 1***

In addition, a Spearman correlation was performed between the independent construct named Perceived Vulnerability and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 2 (F2) of the dependent variable; F2 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Vulnerability and the single index value generated for F2. The correlation reveals that there is a positive and significant correlation between F2 and students' perceptions that they can be victims of a severe data security threat (rho= 0.312, p=0.000, N=371). Moreover, the correlation reveals that there is a positive and significant correlation between F2 and students' perceptions that UKZN can be susceptible to severe data security threat (rho=0.161, p=0.002, N=371). The correlation reveals that there is a positive and significant correlation between F2 and students' perceptions that UKZN faces a growing number of serious data security threats (rho= 0.114, p=0.028, N=371) as shown in Table 4-15 below.

| Correlation | | | Q8 Access to the University network f2 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f2 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 10.1 I could be a victim of a serious information security threat | Correlation Coefficient | .312** |
| | | Sig. (2-tailed) | .000 |
| | | N | 371 |
| | 10.2. UKZN could be subjected to a serious information security threat | Correlation Coefficient | .161** |
| | | Sig. (2-tailed) | .002 |
| | | N | 371 |
| | 10.3. UKZN faces more and more serious information security threats lately. | Correlation Coefficient | .114* |
| | | Sig. (2-tailed) | .028 |
| | | N | 371 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

***Table 4-15: Correlation of Perceived Vulnerability vs Access to the University Network Factor 2***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures to access the university network. As depicted in Table 4-16 below, the regression model significantly predicts the dependent variable outcome (p = 0.000). Student Compliance with Access to the University Network is represented by one regression model. The regression equation that represents the regression model is as follows: F2 access to the university network F2 = Constant + Regression Coefficient = -0.999 - 0.292 * X (where X represents, "I could be a victim of a serious information security threat").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.999 | .224 | | -4.461 | .000 |
| | 10.1 I could be a victim of a serious information security threat | .292 | .057 | .314 | 5.162 | .000 |
| | 10.2. UKZN could be subjected to a serious information security threat | -.068 | .077 | -.061 | -.883 | .378 |
| | 10.3. UKZN faces more and more serious information security threats lately. | .091 | .065 | .081 | 1.385 | .167 |
| a. Dependent Variable: Q8 Access to the University network f2 | | | | | | |

***Table 4-16: Regression of Perceived Vulnerability vs Access to the University Network Factor 2***

In addition, a Spearman correlation was performed between the independent construct named Perceived Vulnerability and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 3 (F3) of the dependent variable; F3 consists of 1 item, the Spearman correlation was performed between Perceived Vulnerability and the single index value generated for F3. The correlation reveals no significant correlation between the two variables.

#### 4.6.2.2. Influence of Perceived Severity on Students' Compliance with Information Security Measures in Place

**a) Descriptive Analysis of the Perceived Severity Responses**

Most students agree (a consolidated percentage of students that agree and strongly agree) that a data security breach at UKZN will pose a significant issue for them (N=375, 70.3%). Furthermore, most students agree that they will lose important data if someone steals their login credentials (N=375, 75%). Moreover, the majority of the students agree that it would be a huge invasion of their privacy if someone steals their login credentials (N=376, 88.3%). Moreover, most students agree that they will be in serious trouble if someone accessed the computer rooms using their student card (N=373, 63.9%). In addition, the majority of the students agree that they will be in serious trouble if someone uses their login details to commit cybercrimes using the university network (N=374, 90.2%). This is corroborated by Table 4-17 below, which displays the mode (i.e. the most frequently chosen answer) for question 11.1 ("An information security breach at UKZN will be a serious problem for me") is 4, indicating that most students agree that a data security breach at UKZN will pose a significant issue for them. Similarly, question 11.2 ("I will lose vital information if my login credentials are stolen") has a mode of 4, indicating that students agree that they will lose important data if someone steals their login credentials. Furthermore, question 11.3 ("My privacy will be seriously violated if my login credentials are stolen") has a mode of 5, indicating that the majority strongly agree that it would be a huge invasion of their privacy if someone steals their login credentials. In Addition, question 11.4 ("I will be in serious trouble if someone access the computer rooms using my student card") has a mode of 4, indicating that students agree that they will be in serious trouble if someone accesses the computer rooms using their student card. Moreover, question 11.5 ("I will be in serious trouble if someone uses my

login details to commit cybercrimes using the university network") has a mode of 5, indicating that most students strongly agree that they will be in serious trouble if someone uses their login details to commit cybercrimes using the university network.

| Statistics | | | | | | |
|---|---|---|---|---|---|---|
| | | 11.1. An information security breach at UKZN will be a serious problem for me | 11.2. I will lose vital information if my login credential are stolen | 11.3. My privacy will be seriously violated if my login credentials are stolen | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network |
| N | Valid | 375 | 375 | 376 | 373 | 374 |
| | Missing | 1 | 1 | 0 | 3 | 2 |
| Mean | | 3.87 | 3.97 | 4.29 | 3.80 | 4.49 |
| Median | | 4.00 | 4.00 | 4.00 | 4.00 | 5.00 |
| Mode | | 4 | 4 | 5 | 4 | 5 |
| Std. Deviation | | .949 | .940 | .802 | 1.011 | .771 |

***Table 4-17: Frequency of Perceived Severity***

**b) Correlation between Perceived Severity and Physical Access to Computer Rooms**

A Spearman correlation was performed between the independent construct named Perceived Severity and the 1st construct from the dependent variable named Student Compliance; the 1st construct in the dependent variable is named Physical Access to Computer Rooms which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 3 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Severity and the single index value generated for F1. The correlation reveals a positive and significant correlation between F1 and students' perceptions that a data security breach at UKZN will pose a significant issue for them (rho= 0.117, p=0.023, N=374). This is the only variable of Perceived Severity that is significant and positively correlated with complying with UKZN Physical Access to Computer Rooms (factor 1) rules, as depicted in Table 4-19 below.

| Correlation | | | Q7 Physical access to computer rooms |
|---|---|---|---|
| Spearman's rho | Q7 Physical access to computer rooms | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 375 |
| | 11.1. An information security breach at UKZN will be a serious problem for me | Correlation Coefficient | .117* |
| | | Sig. (2-tailed) | .023 |
| | | N | 374 |
| | 11.2. I will lose vital information if my login credential are stolen | Correlation Coefficient | .034 |
| | | Sig. (2-tailed) | .507 |
| | | N | 374 |
| | 11.3. My privacy will be seriously violated if my login credentials are stolen | Correlation Coefficient | .012 |
| | | Sig. (2-tailed) | .814 |
| | | N | 375 |
| | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | Correlation Coefficient | -.014 |
| | | Sig. (2-tailed) | .787 |
| | | N | 372 |
| | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | Correlation Coefficient | -.064 |
| | | Sig. (2-tailed) | .215 |
| | | N | 373 |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

***Table 4-19: Correlation of Perceived Severity vs Physical Access to Computer Rooms***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access computer rooms. Table 4-19 below shows that the regression model predicts the dependent variable outcome (p = 0.008). Student Compliance with Physical Access to Computer Rooms is represented by one regression model, the regression equation that represents the regression model is as follows: F1 = Constant + Regression Coefficient = -0.234 + 0.168 * X (where X represents, “An information security breach at UKZN will be a serious problem for me”).

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.234 | .379 | | -.617 | .538 |
| | 11.1. An information security breach at UKZN will be a serious problem for me | .168 | .063 | .158 | 2.659 | .008 |
| | 11.2. I will lose vital information if my login credential are stolen | -.080 | .075 | -.075 | -1.062 | .289 |
| | 11.3. My privacy will be seriously violated if my login credentials are stolen | -.001 | .084 | -.001 | -.014 | .989 |
| | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | -.009 | .058 | -.009 | -.155 | .877 |
| | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | -.011 | .076 | -.009 | -.147 | .883 |
| a. Dependent Variable: Q7 Physical access to computer rooms | | | | | | |

***Table 4-19: Regression of Perceived Severity vs Physical Access to Computer Rooms***

**c) Correlation between Perceived Severity and Access to the University Network**

A Spearman correlation was performed between the independent construct named Perceived Severity and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Severity and the single index value generated for F1. The correlation reveals that there is a negative but significant correlation between F1 and students' perception that they will lose important data if someone steals their login credentials (rho=-0.125, p=0.016, N=371). The correlation further reveals that there is a negative but significant correlation between F1 and students' perceptions that it would be a huge invasion of their privacy if someone steals their login credentials (rho=-0.152, p=0.003, N=372). Finally, the correlation reveals that there is a negative but significant correlation between F1 and students' perceptions that they will be in serious trouble if someone uses their login details to commit cybercrimes using the

University network (rho=-0.179, p=0.001, N=370). These are the only variables of Perceived Severity which are significant and negatively correlated with complying with UKZN Access to the University Network (factor 1) rules, as depicted in Table 4-20 below.

| Correlation | | | Q8 Access to the University network f1 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f1 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 11.1. An information security breach at UKZN will be a serious problem for me | Correlation Coefficient | -.098 |
| | | Sig. (2-tailed) | .060 |
| | | N | 371 |
| | 11.2. I will lose vital information if my login credential are stolen | Correlation Coefficient | -.125* |
| | | Sig. (2-tailed) | .016 |
| | | N | 371 |
| | 11.3. My privacy will be seriously violated if my login credentials are stolen | Correlation Coefficient | -.152** |
| | | Sig. (2-tailed) | .003 |
| | | N | 372 |
| | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | Correlation Coefficient | -.057 |
| | | Sig. (2-tailed) | .276 |
| | | N | 369 |
| | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | Correlation Coefficient | -.179** |
| | | Sig. (2-tailed) | .001 |
| | | N | 370 |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-20: Correlation of Perceived Severity vs Access to the University Network Factor 1***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures to access the university network. As depicted in Table 4-21 below, the regression model significantly predicts the dependent variable outcome (p1 = 0.030). Student Compliance with Access to the University Network is represented by one regression model. The regression equations that describe the regression model is as follows: F1 = 0.127 – 0.165 * X (where X represents "I will be in serious trouble if someone uses my login details to commit cybercrimes using the university network").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 1.127 | .379 | | 2.975 | .003 |
| | 11.1. An information security breach at UKZN will be a serious problem for me | .008 | .063 | .007 | .120 | .904 |
| | 11.2. I will lose vital information if my login credential are stolen | -.077 | .075 | -.072 | -1.024 | .306 |
| | 11.3. My privacy will be seriously violated if my login credentials are stolen | -.062 | .084 | -.049 | -.738 | .461 |
| | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | .041 | .058 | .041 | .695 | .488 |
| | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | -.165 | .076 | -.128 | -2.175 | .030 |
| a. Dependent Variable: Q8 Access to the University network f1 | | | | | | |

***Table 4-21: Regression of Perceived Severity vs Access to the University Network Factor 1***

A Spearman correlation was performed between the independent construct named Perceived Severity and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 2 (F2) of the dependent variable; F2 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Severity and the single index value generated for F2. Table 4-22 reveals that there is a significant and positive correlation between F2 and students' perceptions that they will lose important data if someone steals their login credentials(rho=0.107, p=0.040, N=371). The correlation further reveals that there is a significant and positive correlation between F2 and students' perceptions that they will be in serious trouble if someone accesses the computer rooms using their student card (rho=0.212, p=0.000, N=369). On the contrary, there is a significant but negative correlation between F2 and students' perceptions that they will be in serious trouble if someone uses their login details to commit cybercrimes using the university network (rho=-0.164, p=0.002, N=370). These are the only variables of

Perceived Severity that are significantly correlated with complying with UKZN Access to the University Network (factor 2) rules, as depicted in Table 4-22 below.

| | | | Q8 Access to the University network f2 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f2 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 11.1. An information security breach at UKZN will be a serious problem for me | Correlation Coefficient | .095 |
| | | Sig. (2-tailed) | .066 |
| | | N | 371 |
| | 11.2. I will lose vital information if my login credential are stolen | Correlation Coefficient | .107* |
| | | Sig. (2-tailed) | .040 |
| | | N | 371 |
| | 11.3. My privacy will be seriously violated if my login credentials are stolen | Correlation Coefficient | -.019 |
| | | Sig. (2-tailed) | .719 |
| | | N | 372 |
| | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | Correlation Coefficient | .212** |
| | | Sig. (2-tailed) | .000 |
| | | N | 369 |
| | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | Correlation Coefficient | -.164** |
| | | Sig. (2-tailed) | .002 |
| | | N | 370 |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-22: Correlation of Perceived Severity vs Access to the University Network Factor 2***

Furthermore, a linear regression analysis was carried out to determine the effect of the variables on compliance with measures to access the university network. As depicted in Table 4-23 below, the regression model significantly predicts the dependent variable outcome (p = 0.000). Student Compliance with Access to the University Network is represented by two regression models, the regression equations that represent the regression model are as follows: F2a = Constant + Regression Coefficient = -0.257 + 0.297 * X (where X represents, “I will be in serious trouble if someone access the computer rooms using my student card”) and F2b = Constant + Regression Coefficient = -0.257 - 0.275 * X (where X represents, “I will be in serious trouble if someone uses my login details to commit cybercrimes using the university network”).

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.257 | .364 | | -.708 | .480 |
| | 11.1. An information security breach at UKZN will be a serious problem for me | .102 | .061 | .096 | 1.693 | .091 |
| | 11.2. I will lose vital information if my login credential are stolen | .097 | .072 | .091 | 1.344 | .180 |
| | 11.3. My privacy will be seriously violated if my login credentials are stolen | -.096 | .080 | -.077 | -1.201 | .231 |
| | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | .297 | .056 | .298 | 5.310 | .000 |
| | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | -.275 | .073 | -.211 | -3.765 | .000 |
| a. Dependent Variable: Q8 Access to the University network f2 | | | | | | |

***Table 4-23: Regression of Perceived Severity vs Access to the University Network Factor 2***

A Spearman correlation was performed between the independent construct named Perceived Severity and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 3 (F3) of the dependent variable; F3 consist of 1 item. The Spearman correlation was performed between Perceived Severity and the single index value generated for F3. The correlation reveals that there is a significant and positive correlation between F3 and students' perceptions that they will lose important data if someone steals their login credentials (rho=0.165, p=0.001, N=371). The correlation further reveals that there is a significant and positive correlation between F3 and students' perceptions that it would be a huge invasion of their privacy if someone steals their login credentials (rho=0.178, p=0.001, N=372). Lastly, the correlation reveals that there is a significant and positive correlation between F3 and students perception that they will be in serious trouble if someone access the computer rooms using their student card (rho= 0.106, p=0.0042, N=369) as shown in Table 4-24 below.

| | | | Q8 Access to the University network f3 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f3 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 11.1. An information security breach at UKZN will be a serious problem for me | Correlation Coefficient | .040 |
| | | Sig. (2-tailed) | .443 |
| | | N | 371 |
| | 11.2. I will lose vital information if my login credential are stolen | Correlation Coefficient | .165** |
| | | Sig. (2-tailed) | .001 |
| | | N | 371 |
| | 11.3. My privacy will be seriously violated if my login credentials are stolen | Correlation Coefficient | .178** |
| | | Sig. (2-tailed) | .001 |
| | | N | 372 |
| | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | Correlation Coefficient | .106* |
| | | Sig. (2-tailed) | .042 |
| | | N | 369 |
| | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | Correlation Coefficient | .064 |
| | | Sig. (2-tailed) | .217 |
| | | N | 370 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

***Table 4-24: Correlation of Perceived Severity vs Access to the University Network Factor 3***

Furthermore, a linear regression analysis was carried out to determine the effect of the variables on compliance with measures to access the university network. As depicted in Table 4-25 below the regression model significantly predicts the dependent variable outcome (p = 0.001). Student Compliance with Access to the University Network is represented by one regression model, the regression equation that represents the regression model is as follows: F3 = Constant + Regression Coefficient = -1.023 + 0.273 * X (where X represents, “My privacy will be seriously violated if my login credentials are stolen”).

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -1.023 | .368 | | -2.783 | .006 |
| | 11.1. An information security breach at UKZN will be a serious problem for me | -.119 | .061 | -.112 | -1.940 | .053 |
| | 11.2. I will lose vital information if my login credential are stolen | .166 | .073 | .156 | 2.278 | .023 |
| | 11.3. My privacy will be seriously violated if my login credentials are stolen | .273 | .081 | .218 | 3.358 | .001 |
| | 11.4. I will be in serious trouble if someone access the computer rooms using my student card | .014 | .057 | .015 | .255 | .799 |
| | 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | -.091 | .074 | -.070 | -1.234 | .218 |
| a. Dependent Variable: Q8 Access to the University network f3 | | | | | | |

***Table 4-25: Regression of Perceived Severity vs Access to the University Network Factor 3***

### 4.6.2.3. Influence of Perceived Rewards on Students' Compliance with Information Security Measures in Place

#### a) Descriptive Analysis of the Perceived Rewards Responses

Most students disagree (a consolidated percentage of students that agree and strongly agree) that they would feel rewarded if a friend used their student card to access the LAN. (N=375, 58.8%). Moreover, most students disagree that they would feel rewarded if friends used their LAN credentials to access the university network (N=375, 67.6%). In addition, most students disagree that they benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. (N=375, 44.7%). This is corroborated by Table 4-26 below, which shows the mode (i.e. the most frequently chosen answer) for question 12.1 (I would feel rewarded if a friend uses my LAN credentials to access the university network) is 2, indicating that most students disagree that they would feel rewarded if a friend uses their

LAN credentials to access the university network. Similarly, question 12.2 (I would feel rewarded if a friend uses my LAN credentials to access the university network) has a mode of 2, indicating that most students disagree that they would feel rewarded if a friend uses their LAN credentials to access the university network. In addition, question 12.3 (I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them.) has a mode of 3, indicating that most students do not agree or disagree that sometimes they benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them.

| Statistics | | | | |
|---|---|---|---|---|
| | | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. |
| N | Valid | 375 | 375 | 375 |
| | Missing | 1 | 1 | 1 |
| Mean | | 2.35 | 2.15 | 2.72 |
| Median | | 2.00 | 2.00 | 3.00 |
| Mode | | 2 | 2 | 3 |
| Std. Deviation | | .933 | .885 | 1.159 |

***Table 4-26: Frequency of Perceived Rewards***

**b) Correlation between Perceived Rewards and Physical Access to Computer Rooms**

A Spearman correlation was performed between the independent construct named Perceived Rewards and the 1st construct from the dependent variable named Student Compliance; the 1st construct in the dependent variable is named Physical Access to Computer Rooms which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 3 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Rewards and the single index value generated for F1. The correlation reveals a significant and positive correlation between F1 and students' perceptions that they would feel rewarded if a friend used their student card to access the LAN. (rho=0.341, p=0.000, N=374). Moreover, the Spearman correlation reveals a significant and positive correlation between F1 and students' perceptions that they would feel rewarded if a friend used their LAN credentials to access

the university network (rho= 0.341, p=0.000, N=374). Lastly, the Spearman correlation reveals a significant and positive correlation between F1 and students' perceptions that they benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. (rho= 0.206, p=0.000, N=374), this is corroborated by Table 4-27 below.

| Correlation | | | Q7 Physical access to computer rooms |
|---|---|---|---|
| Spearman's rho | Q7 Physical access to computer rooms | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 375 |
| | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | Correlation Coefficient | .341** |
| | | Sig. (2-tailed) | .000 |
| | | N | 374 |
| | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | Correlation Coefficient | .322** |
| | | Sig. (2-tailed) | .000 |
| | | N | 374 |
| | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | Correlation Coefficient | .206** |
| | | Sig. (2-tailed) | .000 |
| | | N | 374 |
| **. Correlation is significant at 0.01 | | | |

***Table 4-27: Correlation of Perceived Rewards vs Physical Access to Computer Rooms***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access computer rooms. As depicted in Table 4-28 below, the regression model significantly predicts the dependent variable outcome (p = 0.002). **Student Compliance with Physical Access to Computer Rooms is represented by** one regression model, the regression equation that represents the regression model is as follows: F1 = Constant + Regression Coefficient = -1.028 + 0.258 * X (where X represents, "I would feel rewarded if a friend uses my student card to access the LAN").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardised Coefficient | | Standardised Coefficient | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -1.028 | .157 | | -6.556 | .000 |
| | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | .258 | .084 | .241 | 3.054 | .002 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | .084 | .090 | .074 | .927 | .355 |
| | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | .090 | .045 | .104 | 2.007 | .046 |
| a. Dependent Variable: Q7 Physical access to computer rooms | | | | | | |

***Table 4-28: Regression of Perceived Rewards vs Physical Access to Computer Rooms***

### c) Correlation between Perceived Rewards and Access to the University Network

A Spearman correlation was performed between the independent construct named Perceived Rewards and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Rewards and the single index value generated for F1. The correlation reveals that there is a significant and positive correlation between F1 and students' perception that they would feel rewarded if their friend uses their student card to access the LAN (rho=0.204, p=0.000, N=371). Moreover, the correlation reveals that there is a significant and positive correlation between F1 and students' perception that they would feel rewarded if their friend uses their LAN credentials to access the university network (rho= 0.290, p=0.000, N=371). Finally, the correlation also reveals that there is a significant and positive correlation between F1 and student's perception that they benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them (rho= 0.110, p=0.034, N=371), this is depicted in Table 4-29 below.

| | | | Q8 Access to the University network f1 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f1 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | Correlation Coefficient | .204** |
| | | Sig. (2-tailed) | .000 |
| | | N | 371 |
| | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | Correlation Coefficient | .290** |
| | | Sig. (2-tailed) | .000 |
| | | N | 371 |
| | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | Correlation Coefficient | .110* |
| | | Sig. (2-tailed) | .034 |
| | | N | 371 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

***Table 4-29: Correlation of Perceived Rewards vs Access to the University Network Factor 1***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access the university network. As depicted in Table 4-30 below, the regression model significantly predicts the dependent variable outcome ($p = 0.013$). The regression equation that represents the regression model is as follows: F1 = Constant + Regression Coefficient = -0.503+ 0.237 * X (where X represents, “I would feel rewarded if a friend uses my LAN credentials to access the university network”).

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.503 | .165 | | -3.054 | .002 |
| | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | -.053 | .088 | -.050 | -.603 | .547 |
| | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | .237 | .095 | .210 | 2.494 | .013 |
| | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | .044 | .047 | .052 | .947 | .344 |
| a. Dependent Variable: Q8 Access to the University network f1 | | | | | | |

***Table 4-30: Regression of Perceived Rewards vs Access to the University Network Factor 1***

Furthermore, a Spearman correlation was performed between the independent construct named Perceived Rewards and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 2 (F2) of the dependent variable; F2 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Perceived Rewards and the single index value generated for F2. The correlation reveals that there is a significant and positive correlation between F2 and students' perception that they would feel rewarded if a friend uses their student card to access the LAN. (rho=0.236, p=0.000, N=371). The correlation reveals that there is a significant and positive correlation between F2 and students' perception that they would feel rewarded if a friend uses their LAN credentials to access the university network (rho= 0.285, p=0.000, N=371). Lastly, the correlation reveals that there is a significant and positive correlation between F2 and students' perception that they benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them (rho= 0.223, p=0.000, N=371), this is depicted in Table 4-31 below.

| | | | Q8 Access to the University network f2 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f2 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | Correlation Coefficient | .236** |
| | | Sig. (2-tailed) | .000 |
| | | N | 371 |
| | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | Correlation Coefficient | .285** |
| | | Sig. (2-tailed) | .000 |
| | | N | 371 |
| | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | Correlation Coefficient | .223** |
| | | Sig. (2-tailed) | .000 |
| | | N | 371 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-31: Correlation of Perceived Rewards vs Access to the University Network Factor 2***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access the university network. As depicted in Table 4-32 below, the regression model significantly predicts the dependent variable outcome ($p = 0.004$). Student Compliance with Access to the University Network is represented by factor 2 and is significantly correlated to Perceived Rewards. Thus, the regression equation that represents the regression model is as follows: F2 access to the university network F2 = Constant + Regression Coefficient = -0.006+ 0.262 * X (where X represents, "I would feel rewarded if a friend uses my LAN credentials to access the university network").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -1.006 | .158 | | -6.375 | .000 |
| | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | .042 | .085 | .039 | .496 | .620 |
| | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | .262 | .091 | .232 | 2.878 | .004 |
| | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | .125 | .045 | .145 | 2.775 | .006 |
| a. Dependent Variable: Q8 Access to the University network f2 | | | | | | |

***Table 4-32: Regression of Perceived Rewards vs Access to the University Network Factor 2***

A Spearman correlation was performed between the independent construct named Perceived Rewards and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 2 (F2) of the dependent variable; F3 consist of 1 item, a Spearman correlation was performed between Perceived Rewards and the single index value generated for F3. The correlation reveals that there is a significant and negative correlation between F3 and students' perception that they would feel rewarded if a friend uses their student card to access the LAN. (rho=-0.113, p=0.029, N=371). Additionally, the correlation reveals that there is a significant and negative correlation between F3 and students' perception that they would feel rewarded if a friend uses their LAN credentials to access the university network (rho=-0.166, p=0.001, N=371) as depicted in Table 4-33 below.

| | | | Q8 Access to the University network f3 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f3 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | Correlation Coefficient | -.113* |
| | | Sig. (2-tailed) | .029 |
| | | N | 371 |
| | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | Correlation Coefficient | -.166** |
| | | Sig. (2-tailed) | .001 |
| | | N | 371 |
| | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | Correlation Coefficient | -.092 |
| | | Sig. (2-tailed) | .075 |
| | | N | 371 |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-33: Correlation of Perceived Rewards vs Access to the University Network Factor 3***

A linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access the university network. As depicted in Table 4-41 below, the regression model does not significantly predict the dependent variable outcome ($p > 0.050$).

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | .377 | .167 | | 2.262 | .024 |
| | 12.1. I would feel rewarded if a friend uses my student card to access the LAN. | .045 | .089 | .042 | .505 | .614 |
| | 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | -.131 | .096 | -.116 | -1.363 | .174 |
| | 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | -.074 | .047 | -.086 | -1.557 | .120 |

***Table 4-34: Regression of Perceived Rewards vs Access to the University Network Factor 3***

### 4.6.3. Research Question 3: What are the Effects of Coping Appraisal on Students' Compliance with the Information Security Measures within the University?

The participants answered questions based on the Protection Motivation Theory construct (Coping Appraisal) from this research's conceptual model. The Coping Appraisal construct includes Response Efficacy, Self-Efficacy and Response Cost. The following are the responses to all the questions using a Likert scale ranging from "Strongly Agree" (5) to "Strongly Disagree" (1). This is also displayed in Appendix G.

#### 4.6.3.1. Influence of Response Efficacy on Students' Compliance with Information Security Measures in Place

**a) Descriptive Analysis of the Response Efficacy Responses**

Most students agree (a consolidated percentage of students that agree and strongly agree) that NOT sharing their LAN login details prevents or reduces the chances of identity theft (N=376, 91%). Furthermore, most students agree that NOT sharing their student cards helps to reduce security breaches (N=376, 87%). In addition, most students agree that if they comply with information security policies, Information Systems security breaches will be scarce. (N=376, 8080%). This is corroborated by Table 4-35 below, which shows the mode (i.e. the most frequently chosen answer) for question 13.1 ("I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft") is 5, indicating that the majority of students strongly agree that NOT sharing their LAN login details prevents or reduces chances of identity theft. Similarly, question 13.2 ("I believe that NOT sharing my student card helps to reduce security breaches") has a mode is 5, indicating that the majority of students strongly agree that NOT sharing their student card helps to reduce security breaches. In addition, question 13.3 ("If I comply with information security policies, Information Systems security breaches will be scarce") has a mode of 4, indicating that most students agree that if they comply with information security policies, Information Systems security breaches will be scarce.

| Statistics | | | | |
|---|---|---|---|---|
| | | 13.1. I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft. | 13.2. I believe that NOT sharing my student card helps to reduce security breaches. | 13.3. If I comply with information security policies, Information Systems security breaches will be scarce. |
| N | Valid | 376 | 376 | 376 |
| | Missing | 0 | 0 | 0 |
| Mean | | 4.40 | 4.28 | 4.17 |
| Median | | 5.00 | 4.00 | 4.00 |
| Mode | | 5 | 5 | 5 |
| Std. Deviation | | .756 | .809 | .833 |

***Table 4-35: Frequency of Response Efficacy***

**b) Correlation between Response Efficacy and Physical Access to Computer Rooms**

A Spearman correlation was performed between the independent construct named Response Efficacy and the 1st construct from the dependent variable named Student Compliance; the 1st construct in the dependent variable is named Physical Access to Computer Rooms which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 3 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Response Efficacy and the single index value generated for F1. The correlation reveals that there is a negative but significant correlation between F1 and students' perceptions that NOT sharing their LAN login details prevents or reduces chances of identity theft (rho= -.133, p=0.010, N=375). The correlation further reveals that there is a negative but significant correlation between F1 and students' perceptions that NOT sharing their student card helps to reduce security breaches (rho= -.169, p=0.001, N=375) as depicted in Table 4-36 below.

| Correlation | | | Q7 Physical access to computer rooms |
|---|---|---|---|
| Spearman's rho | Q7 Physical access to computer rooms | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 375 |
| | 13.1. I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft. | Correlation Coefficient | -.133* |
| | | Sig. (2-tailed) | .010 |
| | | N | 375 |
| | 13.2. I believe that NOT sharing my student card helps to reduce security breaches. | Correlation Coefficient | -.169** |
| | | Sig. (2-tailed) | .001 |
| | | N | 375 |
| | 13.3. If I comply with information security policies, Information Systems security breaches will be scarce. | Correlation Coefficient | -.093 |
| | | Sig. (2-tailed) | .071 |
| | | N | 375 |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-36: Correlation of Response Efficacy vs Physical Access to Computer Rooms***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access computer rooms. As depicted in Table 4-37 below, the regression model significantly predicts the dependent variable outcome ($p = 0.043$). Student Compliance with Physical Access to Computer Rooms is represented by two regression models because factor analysis revealed that there is one factor (F1) representing compliance to access to the university network, the regression equation that represents the regression model is as follows: F1 = Constant + Regression Coefficient = 0.756 - 0.206 * X (where X represents, “I believe that NOT sharing my student card helps to reduce security breaches”).

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | .756 | .328 | | 2.306 | .022 |
| | 13.1. I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft. | .051 | .100 | .038 | .509 | .611 |
| | 13.2. I believe that NOT sharing my student card helps to reduce security breaches. | -.206 | .101 | -.166 | -2.033 | .043 |
| | 13.3. If I comply with information security policies, Information Systems security breaches will be scarce. | -.024 | .078 | -.020 | -.306 | .759 |
| a. Dependent Variable: Q7 Physical access to computer rooms | | | | | | |

***Table 4-37: Regression of Response Efficacy vs Physical Access to Computer Rooms***

### c) Correlation between Response Efficacy and Access to the University Network

A Spearman correlation was performed between the independent construct named Response Efficacy and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Response Efficacy and the single index value generated for F1. The correlation reveals that there is a negative but significant correlation between F1 and students' perception that NOT sharing their LAN login details prevents or reduces chances of identity theft (rho= -0.266, p=0.000, N=372). The correlation reveals that there is a negative but significant correlation between F1 and students' perception that NOT sharing their student card helps to reduce security breaches (rho= -0.228, p=0.000, N=372). Lastly, the correlation reveals that there is a negative but significant correlation between F1 and students' perception that if they comply with information security policies, Information Systems security breaches will be scarce (rho= -0.207, p=0.000, N=372). These are the only variables of Response Efficacy that are significantly and negatively correlated with complying with UKZN Access to the University Network (factor 1) rules as depicted in Table 4-38 below.

| Correlations | | | Q8 Access to the University network f1 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f1 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 13.1. I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft. | Correlation Coefficient | -.266** |
| | | Sig. (2-tailed) | .000 |
| | | N | 372 |
| | 13.2. I believe that NOT sharing my student card helps to reduce security breaches. | Correlation Coefficient | -.228** |
| | | Sig. (2-tailed) | .000 |
| | | N | 372 |
| | 13.3. If I comply with information security policies, Information Systems security breaches will be scarce. | Correlation Coefficient | -.207** |
| | | Sig. (2-tailed) | .000 |
| | | N | 372 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-38: Correlation of Response Efficacy vs Access to the University Network Factor 1***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures to access the university network. As depicted in Table 4-39 below, the regression model significantly predicts the dependent variable outcome ($p = 0.025$). Student Compliance with Access to the University Network is represented by factor 1 of access to the university network and is significantly correlated to response efficacy. Thus, the regression equation that represents the regression model is as follows: F1 = Constant + Regression Coefficient = 1.435 - 0.221 * X (where X represents, “I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft”).

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 1.435 | .329 | | 4.356 | .000 |
| | 13.1. I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft. | -.221 | .098 | -.165 | -2.257 | .025 |
| | 13.2. I believe that NOT sharing my student card helps to reduces security breaches. | -.057 | .099 | -.045 | -.573 | .567 |
| | 13.3. If I comply with information security policies, Information Systems security breaches will be scarce. | -.052 | .077 | -.043 | -.680 | .497 |
| a. Dependent Variable: Q8 Access to the University network f1 | | | | | | |

***Table 4-39: Regression of Response Efficacy vs Access to the University Network Factor 1***

A Spearman correlation was performed between the independent construct named Response Efficacy and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 2 (F2) of the dependent variable; F2 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Response Efficacy and the single index value generated for F2. The correlation reveals revealed that there is no significant correlation between F2 and the Response Efficacy construct. On the contrary, a Spearman correlation was performed between the independent construct named Response Efficacy and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 3 (F3) of the dependent variable; F3 consists of 1 item, the Spearman correlation was performed between Response Efficacy and the single index value generated for F3. The correlation reveals revealed that there is a significant positive correlation between F3 and students' perception that NOT sharing their LAN login details prevents or reduces chances of identity theft (rho= 0.175, p=0.001, N=372). Moreover, the correlation reveals revealed that there is a significant positive correlation between F3 and students' perception that NOT sharing their student card helps to reduce security breaches (rho= 0.138, p=0.008, N=372). Finally, the correlation reveals that there is a

significant positive correlation between F3 and students' perception that if they comply with information security policies, Information Systems security breaches will be scarce (rho= 0.177, p=0.001, N=372) as depicted in Table 4-40 below.

| Correlation | | | Q8 Access to the University network f3 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f3 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 13.1. I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft. | Correlation Coefficient | .175** |
| | | Sig. (2-tailed) | .001 |
| | | N | 372 |
| | 13.2. I believe that NOT sharing my student card helps to reduces security breaches. | Correlation Coefficient | .138** |
| | | Sig. (2-tailed) | .008 |
| | | N | 372 |
| | 13.3. If I comply with information security policies, Information Systems security breaches will be scarce. | Correlation Coefficient | .177** |
| | | Sig. (2-tailed) | .001 |
| | | N | 372 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-40: Correlation of Response Efficacy vs Access to the University Network Factor 3***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access computer rooms. As depicted in Table 4-41 below the regression model does not significantly predicts the dependent variable outcome ($p > 0.050$).

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -1.047 | .333 | | -3.143 | .002 |
| | 13.1. I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft. | .154 | .099 | .115 | 1.555 | .121 |
| | 13.2. I believe that NOT sharing my student card helps to reduces security breaches. | -.044 | .100 | -.036 | -.444 | .657 |
| | 13.3. If I comply with information security policies, Information Systems security breaches will be scarce. | .134 | .078 | .111 | 1.721 | .086 |
| a. Dependent Variable: Q8 Access to the University network f3 | | | | | | |

*Table 4-41: Regression of Response Efficacy vs Access to the University Network Factor 3*

### 4.6.3.2. Influence of Self-efficacy on Students' Compliance with Information Security Measures in Place

#### a) Descriptive Analysis of the Self-efficacy Responses

The majority of students agree (a consolidated percentage of students that agree and strongly agree) that they are capable of complying with UKZN information security measures by themselves (N=376, 80.6%). Furthermore, most students disagree that they need assistance complying with UKZN data security measures (N=376, 42.8%). In addition, most students disagree that they are not confident enough with complying with UKZN data security measures (N=375, 52.3%). This is corroborated by Appendix E and Table 4-42 below that shows the mode (i.e. the most frequently chosen answer) for question 14.1 ("I can comply with UKZN information security measures by myself") is 4 indicating that most students agree that they are capable of complying with UKZN information security measures by themselves. Contrarily, question 14.2 ("I need assistance to comply with UKZN information security measures") has a mode is 2 indicating that most students disagree that they need assistance complying with UKZN data security measures. In addition, question 14.3 ("I am not confident enough to comply with UKZN information security measures") has a mode of 2 indicating that most students disagree that they are not confident enough with complying with UKZN data security measures.

| Statistics | | | | |
|---|---|---|---|---|
| | | 14.1. I can comply with UKZN information security measures by myself | 14.2. I need assistance to comply with UKZN information security measures | 14.3. I am not confident enough to comply with UKZN information security measures |
| N | Valid | 376 | 376 | 375 |
| | Missing | 0 | 0 | 1 |
| Mean | | 4.03 | 2.82 | 2.59 |
| Median | | 4.00 | 3.00 | 2.00 |
| Mode | | 4 | 2 | 2 |
| Std. Deviation | | .796 | 1.027 | 1.032 |

*Table 4-42: Frequency of Self-Efficacy*

**b) Correlation between Self-efficacy and Physical Access to Computer Rooms**

A Spearman correlation was performed between the independent construct named Self-efficacy and the 1st construct from the dependent variable named Student Compliance; the 1st construct in the dependent variable is named Physical Access to Computer Rooms which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 3 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Self-efficacy and the single index value generated for F1. The correlation reveals that there is no significant correlation between F1 and the Self-efficacy construct as depicted in Appendix F. Subsequently, a linear regression analysis was not conducted to assess the effect of the two variables.

**c) Correlation between Self-efficacy and Access to the University Network**

A Spearman correlation was performed between the independent construct named Self-efficacy and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Self-efficacy and the single index value generated for F1. The correlation reveals that there is a negative and significant correlation between F1 and students' perception that they are capable of complying with UKZN information security measures by themselves (rho= -0.157, p=0.002, N=372).The results reveal there is also a significant and positive correlation between F1 and students' perceptions that they need assistance complying with UKZN data security measures (rho= 0.104, p=0.046, N=372). Lastly, the correlation reveals that there is a significant and positive correlation between F1 and students' perception that perceptions that they are not confident enough with complying with UKZN data security measures (rho= 0.185, p=0.000, N=371) as depicted in Table 4-43 below.

| | | | Q8 Access to the University network f1 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f1 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 14.1. I can comply with UKZN information security measures by myself | Correlation Coefficient | -.157** |
| | | Sig. (2-tailed) | .002 |
| | | N | 372 |
| | 14.2. I need assistance to comply with UKZN information security measures | Correlation Coefficient | .104* |
| | | Sig. (2-tailed) | .046 |
| | | N | 372 |
| | 14.3. I am not confident enough to comply with UKZN information security measures | Correlation Coefficient | .185** |
| | | Sig. (2-tailed) | .000 |
| | | N | 371 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

***Table 4-43: Correlation of Self-Efficacy vs Access to the University Network Factor 1***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access the university network. As depicted in Table 4-44 below, the regression model significantly predicts the dependent variable outcome ($p = 0.009$). Compliance to access to the university network is significantly correlated to Self-efficacy. Thus, the regression equation that represents the regression model is as follows: $F1 = 0.157 + 0.152* X$ (where X represents, "I am not confident enough to comply with UKZN information security measures").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | .157 | .358 | | .439 | .661 |
| | 14.1. I can comply with UKZN information security measures by myself | -.122 | .067 | -.097 | -1.812 | .071 |
| | 14.2. I need assistance to comply with UKZN information security measures | -.020 | .059 | -.021 | -.343 | .732 |
| | 14.3. I am not confident enough to comply with UKZN information security measures | .152 | .058 | .157 | 2.613 | .009 |
| a. Dependent Variable: Q8 Access to the University network f1 | | | | | | |

***Table 4-44: Regression of Self-Efficacy vs Access to the University Network Factor 1***

A Spearman correlation was performed between the independent construct named Self-efficacy and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 2 (F2) of the dependent variable; F2 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Self-efficacy and the single index value generated for F2. The correlation reveals that there is a significant and positive correlation between F2 and students' perceptions that they need assistance complying with UKZN data security measures (rho= 0.148, p=0.004, N=372) as depicted in Table 4-45 below.

| | | | Q8 Access to the University network f2 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f2 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 14.1. I can comply with UKZN information security measures by myself | Correlation Coefficient | -.005 |
| | | Sig. (2-tailed) | .924 |
| | | N | 372 |
| | 14.2. I need assistance to comply with UKZN information security measures | Correlation Coefficient | .148** |
| | | Sig. (2-tailed) | .004 |
| | | N | 372 |
| | 14.3. I am not confident enough to comply with UKZN information security measures | Correlation Coefficient | .091 |
| | | Sig. (2-tailed) | .082 |
| | | N | 371 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-45: Correlation of Self-Efficacy vs Access to the University Network Factor 2***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access the university network. As depicted in Table 4-46 below, the regression model significantly predicts the dependent variable outcome (p = 0.015). Compliance to access to the university network is significantly correlated to Self-efficacy. Thus, the regression equation that represent the regression model is as follows: F2 =-0.899 + 0.145* X (where X represents, "I need assistance to comply with UKZN information security measures").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.899 | .361 | | -2.489 | .013 |
| | 14.1. I can comply with UKZN information security measures by myself | .108 | .068 | .086 | 1.599 | .111 |
| | 14.2. I need assistance to comply with UKZN information security measures | .145 | .060 | .149 | 2.432 | .015 |
| | 14.3. I am not confident enough to comply with UKZN information security measures | .021 | .059 | .021 | .355 | .722 |
| a. Dependent Variable: Q8 Access to the University network f2 | | | | | | |

***Table 4-46: Regression of Self-Efficacy vs Access to the University Network Factor 2***

A Spearman correlation was performed between the independent construct named Self-efficacy and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 3 (F3) of the dependent variable; F3 consists of 1 item, the Spearman correlation was performed between Self-efficacy and the single index value generated for F3. The correlation reveals that there is a significant and positive correlation between F3 and students' perception that they can comply with UKZN information security measures by myself (rho= 0.148, p=0.000, N=372) as depicted in Table 4-47 below.

| | | | Q8 Access to the University network f3 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f3 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 14.1. I can comply with UKZN information security measures by myself | Correlation Coefficient | .214** |
| | | Sig. (2-tailed) | .000 |
| | | N | 372 |
| | 14.2. I need assistance to comply with UKZN information security measures | Correlation Coefficient | -.044 |
| | | Sig. (2-tailed) | .396 |
| | | N | 372 |
| | 14.3. I am not confident enough to comply with UKZN information security measures | Correlation Coefficient | -.069 |
| | | Sig. (2-tailed) | .183 |
| | | N | 371 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-47: Correlation of Self-Efficacy vs Access to the University Network Factor 3***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access the university network. As depicted in Table 4-48 below, the regression model significantly predicts the dependent variable outcome (p = 0.000). Compliance to access to the university network is significantly correlated to Self-efficacy. Thus, the regression equation that represents the regression model is as follows: F3 =-1.151+ 0.256* X (where X represents, "I can comply with UKZN information security measures by myself").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -1.151 | .359 | | -3.209 | .001 |
| | 14.1. I can comply with UKZN information security measures by myself | .256 | .067 | .204 | 3.810 | .000 |
| | 14.2. I need assistance to comply with UKZN information security measures | .036 | .059 | .037 | .615 | .539 |
| | 14.3. I am not confident enough to comply with UKZN information security measures | .006 | .058 | .006 | .103 | .918 |
| a. Dependent Variable: Q8 Access to the University network f3 | | | | | | |

***Table 4-48: Regression of Self-Efficacy vs Access to the University Network Factor 3***

### 4.6.3.3. Influence of Response Cost on Students' Compliance with Information Security Measures in Place

#### a) Descriptive Analysis of the Response Cost Responses

Most students disagree (a consolidated percentage of students that agree and strongly agree) that complying with data security measures is an inconvenience to them (N=376, 61.7%). Furthermore, most students disagree that it is time-consuming to comply with information security measures (N=376, 57.2%). In addition, most students disagree that complying with information security measures requires a lot of effort other than time (N=376, 53,4%). This is corroborated by Table 4-49 below which shows the mode (i.e. the most frequently chosen answer) for question 15.1 ("Complying with information security measures is an inconvenience to me") is 2 indicating that most students disagree that complying with data security measures is an inconvenience to them. Similarly, question 15.2 ("Complying with information security measures is time consuming") has

a mode of 2 indicating that most students disagree that it is time-consuming to comply with information security measures. In addition, question 15.3 ("complying with information security measures requires a lot of effort other than time") has a mode of 2 indicating that most students disagree that complying with information security measures requires a lot of effort other than time.

| Statistics | | | | |
|---|---|---|---|---|
| | | 15.1. Complying with information security measures is an inconvenience to me | 15.2. Complying with information security measures is time consuming | 15.3. Complying with information security measures requires a lot of effort other than time |
| N | Valid | 376 | 376 | 376 |
| | Missing | 0 | 0 | 0 |
| Mean | | 2.41 | 2.53 | 2.56 |
| Median | | 2.00 | 2.00 | 2.00 |
| Mode | | 2 | 2 | 2 |
| Std. Deviation | | .942 | 1.050 | 1.077 |

***Table 4-49: Frequency of Response Cost***

**b) Correlation between Response Cost and Physical Access to Computer Rooms**

A Spearman correlation was performed between the independent construct named Response Cost and the 1st construct from the dependent variable named Student Compliance; the 1st construct in the dependent variable is named Physical Access to Computer Rooms which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 3 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Response Cost and the single index value generated for F1. The correlation reveals that there is no significant correlation between Physical Access to Computer Rooms and Response Cost construct, this is shown in Appendix H. Subsequently, a linear regression analysis was not conducted to assess the effect of the two variables.

**c) Correlation between Response Cost and Access to the University Network**

A Spearman correlation was performed between the independent construct named Response Cost and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Response Cost and the single index value

generated for F1. The correlation reveals that there is a significant and positive correlation between F1 and students' perception that complying with data security measures is an inconvenience to them (rho= 0.227, p=0.000, N=372). Moreover, the correlation reveals that there is a significant and positive correlation between F1 and students' perception that complying with information security measures is time-consuming (rho= 0.165, p=0.001, N=372). Lastly, the correlation reveals that there is a significant and positive correlation between F1 and students' perception that complying with information security measures requires a lot of effort other than time (rho= 0.115, p=0.027, N=372), this is depicted in Table 4-50 below.

| | | | Q8 Access to the University network f1 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f1 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 15.1. Complying with information security measures is an inconvenience to me | Correlation Coefficient | .227** |
| | | Sig. (2-tailed) | .000 |
| | | N | 372 |
| | 15.2. Complying with information security measures is time consuming | Correlation Coefficient | .164** |
| | | Sig. (2-tailed) | .001 |
| | | N | 372 |
| | 15.3. Complying with information security measures requires a lot of effort other than time | Correlation Coefficient | .115* |
| | | Sig. (2-tailed) | .027 |
| | | N | 372 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

***Table 4-50: Correlation of Response Cost vs Access to the University Network Factor 1***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access the university network. As depicted in Table 4-51 below, the regression model significantly predicts the dependent variable outcome (p = 0.001). Student Compliance with Access to the University Network is represented by one regression model from factor 1. Thus, the regression equation that represents the regression model is as follows: F1 = (Constant) + Regression Coefficient = -0.579 + 0.231 * X (where X represents, "Complying with information security measures is an inconvenience to me").

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.579 | .152 | | -3.801 | .000 |
| | 15.1. Complying with information security measures is an inconvenience to me | .231 | .071 | .218 | 3.252 | .001 |
| | 15.2. Complying with information security measures is time consuming | .053 | .076 | .056 | .706 | .481 |
| | 15.3. Complying with information security measures requires a lot of effort other than time | -.044 | .068 | -.047 | -.649 | .516 |
| a. Dependent Variable: Q8 Access to the University network f1 | | | | | | |

***Table 4-51: Regression of Response Cost vs Access to the University Network Factor 1***

Furthermore, A Spearman correlation was performed between the independent construct named Response Cost and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 2 (F2) of the dependent variable; F2 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Response Cost and the single index value generated for F2. The correlation reveals that there is a significant and negative correlation between F2 and students' perception that it is time-consuming to comply with information security measures (rho= -0.106, p=0.040, N=372). The correlation reveals that there is a significant and negative correlation between F2 and students' perception that complying with information security measures requires a lot of effort other than time (rho= -0.119, p=0.022, N=372), this is depicted in Table 4-52 below. Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access computer rooms. As depicted in Appendix F, the regression model does not significantly predict the dependent variable outcome ($p > 0.050$).

| Correlations | | | Q8 Access to the University network f2 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f2 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 15.1. Complying with information security measures is an inconvenience to me | Correlation Coefficient | .046 |
| | | Sig. (2-tailed) | .371 |
| | | N | 372 |
| | 15.2. Complying with information security measures is time consuming | Correlation Coefficient | .106* |
| | | Sig. (2-tailed) | .040 |
| | | N | 372 |
| | 15.3. Complying with information security measures requires a lot of effort other than time | Correlation Coefficient | .119* |
| | | Sig. (2-tailed) | .022 |
| | | N | 372 |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-52: Correlation of Response Cost vs Access to the University Network Factor 2***

A Spearman correlation was performed between the independent construct named Response Cost and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 3 (F3) of the dependent variable; F3 consists of 1 item, the Spearman correlation was performed between Response Cost and the single index value generated for F3. The correlation reveals that there is a significant and negative correlation between F3 and students' perception that complying with data security measures is an inconvenience to them (rho= -0.148, p=0.004, N=372). Moreover, the correlation reveals that there is a significant that there is a significant and negative correlation between F3 and students' perception that it is time-consuming to comply with information security measures (rho= -0.128, p=0.014, N=372). Finally, the correlation reveals that there is a significant that there is a significant and negative correlation between F3 and students' perception that complying with information security measures requires a lot of effort other than time (rho= -0.143, p=0.006, N=372), this is depicted in Table 4-53 below. In addition, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access computer rooms. As depicted in Appendix F, the regression model does not significantly predict the dependent variable outcome ($p > 0.050$).

| Correlations | | | Q8 Access to the University network f3 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f3 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 15.1. Complying with information security measures is an inconvenience to me | Correlation Coefficient | -.148** |
| | | Sig. (2-tailed) | .004 |
| | | N | 372 |
| | 15.2. Complying with information security measures is time consuming | Correlation Coefficient | -.128* |
| | | Sig. (2-tailed) | .014 |
| | | N | 372 |
| | 15.3. Complying with information security measures requires a lot of effort other than time | Correlation Coefficient | -.143** |
| | | Sig. (2-tailed) | .006 |
| | | N | 372 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

***Table 4-53: Correlation of Response Cost vs Access to the University Network Factor 2***

### 4.6.4. Research Question 4: What are the Challenges Faced by Students in their Compliance with the Information Security Measures within the University?

**a) Descriptive Analysis of the Challenges Towards Students' Compliance Responses**

Most students disagree (a consolidated percentage of students that agree and strongly agree) that they do not have the required IT skills to comply with UKZN data security control (N=375, 61,5%). Furthermore, most students disagree that they do not have enough cybersecurity knowledge to comply with UKZN information security measures in place (N=376, 45.2%). Moreover, most students disagree that they do not know how to change the password that they use to access the UKZN network (N=376, 78.4%). Furthermore, more than half of students disagree that they are not aware of ICS policy with regard to the use of passwords (N=376, 53.2%). In addition, most students disagree that they are not aware of ICS/UKZN policy with regard to accessing computer rooms (N=298, 57.7%). Furthermore, more than half of the students disagree that they are not informed about the latest phishing scams (N=376, 52.4%). Additionally, most students disagree that there are not informed about the latest cybersecurity crimes (N=374, 47%). This is corroborated by Table 4-53 below that shows the mode (i.e. the most frequently chosen answer) for question 16.1 ("I do not have the required IT skills to comply with UKZN information security measures") is 2 indicating that most students disagree that

they do not have the required IT skills to comply with UKZN data security controls. Moreover, question 16.2 ("I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place") has a mode is 2 indicating that most students disagree that they do not have enough cybersecurity knowledge to comply with UKZN information security measures in place. Furthermore, question 16.3 ("I do not know how to change the password that I use to access the UKZN network") has a mode of 2 indicating that most students disagree that they do not know how to change the password they use to access the UKZN network. Similarly, question 16.4 ("I am not aware of ICS policy with regard to the use of password") has a mode of 2 indicating that most students disagree that they are not aware of ICS policy regarding to the use of passwords. In addition, question 16.5 ("I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs)") has a mode of 2 indicating that students disagree that they are not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs). Moreover, question 16.6 ("I am not informed about the latest phishing scams (email scams)") has a mode of 2 indicating that students disagree that they are not informed about the latest phishing scams (email scams). Additionally, question 16.7 ("I am not informed about the latest cybersecurity crimes") has a mode of 2 indicating that students agree that they are not informed about the latest cybersecurity crimes. These responses indicate that students are aware of the latest cybersecurity crimes that take place.

| Statistics | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 16.1. I do not have the required IT skills to comply with UKZN information security measures | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | 16.3. I do not know how to change the password that I use to access the UKZN network | 16.4. I am not aware of ICS policy with regard to the use of password | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | 16.6. I am not informed about the latest phishing scams (email scams) | 16.7. I am not informed about the latest cybersecurity crimes |
| N | Valid | 375 | 376 | 375 | 376 | 376 | 376 | 374 |
| | Missing | 1 | 0 | 1 | 0 | 0 | 0 | 2 |
| Mean | | 2.42 | 2.72 | 2.06 | 2.65 | 2.50 | 2.65 | 2.79 |
| Median | | 2.00 | 3.00 | 2.00 | 2.00 | 2.00 | 2.00 | 3.00 |
| Mode | | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Std. Deviation | | 1.069 | 1.149 | 1.014 | 1.131 | 1.093 | 1.237 | 1.257 |

***Table 4-54: Frequency of Challenges Towards Students' Compliance***

**b) Correlation between Challenges Towards Students' Compliance and Physical Access to Computer Rooms**

A Spearman correlation was performed between the independent construct named Challenges Towards Student Compliance and the 1st construct from the dependent variable named Student Compliance; the 1st construct in the dependent variable is named Physical Access to Computer Rooms which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 3 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between the Challenges Towards Student Compliance and the single index value generated for F1. The correlation reveals that there is a significant and positive correlation between F1 and students' perceptions that they do not have enough cybersecurity knowledge to comply with UKZN information security measures in place (rho= 0.186, p=0.000, N=375). The correlation reveals that there is a significant and positive correlation between F1 and students' perceptions that they do not know how to change the password that they use to access the UKZN network (rho= 0.131, p=0.011, N=374). The correlation further reveals that there is a significant and positive correlation between F1 and students' perceptions that they are not aware of ICS policy with regard to the use of passwords (rho= 0.169, p=0.001, N=375). Lastly, the correlation reveals that there is a significant and positive correlation between F1 and students' perceptions that they are not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) (rho= 0.225, p=0.000, N=375) as depicted in Appendix H.

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place to access computer rooms. As depicted in Table 4.53 below, the regression model significantly predicts the dependent variable outcome (p = 0.006). Student Compliance with Physical Access to Computer Rooms is represented by one regression model. Thus, the regression equation that represents the regression model is as follows: F1 = -0.601+ 0.172* X (where X represents, "I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place").

**c) Correlation between Challenges Towards Students' Compliance and Access to the University Network**

A Spearman correlation was performed between the independent construct named Challenges Towards Student Compliance and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 1 (F1) of the dependent variable; F1 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Challenges Towards Student Compliance and the single index value generated for F1. The correlation reveals that there is a significant and positive correlation between F1 and students' perception that they do not know how to change the password that they use to access the UKZN network (rho=0.147, p=0.005, N=371). Moreover, the correlation reveals that there is a significant and positive correlation between F1 and students' perception that they are not aware of ICS policy regarding password use (rho=0.130, p=0.012, N=372). The correlation further reveals that there is a significant and positive correlation between F1 and students' perception that they are not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) (rho=0.148, p=0.004, N=371). Lastly the correlation reveals that there is a significant and positive correlation between F1 and students' perception that they are not informed about the latest phishing scams (email scams) (rho=0.151, p=0.004, N=372) as depicted in Table 4-55 below.

| | | | Q8 Access to the University network f1 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f1 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 16.1. I do not have the required IT skills to comply with UKZN information security measures | Correlation Coefficient | .050 |
| | | Sig. (2-tailed) | .336 |
| | | N | 371 |
| | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | Correlation Coefficient | -.003 |
| | | Sig. (2-tailed) | .960 |
| | | N | 372 |
| | 16.3. I do not know how to change the password that I use to access the UKZN network | Correlation Coefficient | .147** |
| | | Sig. (2-tailed) | .005 |
| | | N | 371 |
| | 16.4. I am not aware of ICS policy with regard to the use of password | Correlation Coefficient | .130* |
| | | Sig. (2-tailed) | .012 |
| | | N | 372 |
| | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | Correlation Coefficient | .148** |
| | | Sig. (2-tailed) | .004 |
| | | N | 372 |
| | 16.6. I am not informed about the latest phishing scams (email scams) | Correlation Coefficient | .151** |
| | | Sig. (2-tailed) | .004 |
| | | N | 372 |
| | 16.7. I am not informed about the latest cybersecurity crimes | Correlation Coefficient | .091 |
| | | Sig. (2-tailed) | .080 |
| | | N | 370 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

***Table 4-55: Correlation of Challenges Towards Students' Compliance vs Access to the University Network Factor 1***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place for the university network. As depicted in Table 4-56 below, the regression model significantly predicts the dependent variable outcome (p = 0.042). Student Compliance with Access to the University Network is represented by one regression model F1= (Constant) + Regression Coefficient = -0.376 + 0.150 * X (where X represents, "I am not informed about the latest phishing scams (email scams)").

| Coefficientsa | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.376 | .172 | | -2.181 | .030 |
| | 16.1. I do not have the required IT skills to comply with UKZN information security measures | .031 | .067 | .034 | .465 | .642 |
| | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | -.111 | .062 | -.133 | -1.808 | .071 |
| | 16.3. I do not know how to change the password that I use to access the UKZN network | .110 | .055 | .116 | 1.988 | .048 |
| | 16.4. I am not aware of ICS policy with regard to the use of password | .065 | .058 | .076 | 1.122 | .263 |
| | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | .016 | .062 | .018 | .262 | .794 |
| | 16.6. I am not informed about the latest phishing scams (email scams) | .150 | .073 | .191 | 2.045 | .042 |
| | 16.7. I am not informed about the latest cybersecurity crimes | -.088 | .070 | -.114 | -1.259 | .209 |
| a. Dependent Variable: Q8 Access to the University network f1 | | | | | | |

***Table 4-56: Regression of Challenges Towards Students' Compliance vs Access to the University Network Factor 1***

A Spearman correlation was performed between the independent construct named Challenges Towards Student Compliance and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 2 (F2) of the dependent variable; F2 consists of 4 items that have been conflated into a single index via factor analysis. The Spearman correlation was performed between Challenges Towards Student Compliance and the single index value generated for F2. The correlation reveals that there is a significant and positive correlation between F2 and students' perception that they do not have the required IT skills to comply with UKZN data security controls (rho= 0.143, p=0.006, N=371). Furthermore, the correlation reveals that there is a

significant and positive correlation between F2 and students' perception that they do not have enough cybersecurity knowledge to comply with UKZN information security measures in place (rho= 0.187, p=0.000, N=372). Finally, the correlation reveals that there is a significant and positive correlation between F2 and students' perception that they do not know how to change the password that I use to access the UKZN network (rho=0.249, p=0.000, N=371); This is depicted in Table 4-57 below.

| | | | Q8 Access to the University network f2 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f2 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 16.1. I do not have the required IT skills to comply with UKZN information security measures | Correlation Coefficient | .143** |
| | | Sig. (2-tailed) | .006 |
| | | N | 371 |
| | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | Correlation Coefficient | .187** |
| | | Sig. (2-tailed) | .000 |
| | | N | 372 |
| | 16.3. I do not know how to change the password that I use to access the UKZN network | Correlation Coefficient | .249** |
| | | Sig. (2-tailed) | .000 |
| | | N | 371 |
| | 16.4. I am not aware of ICS policy with regard to the use of password | Correlation Coefficient | .101 |
| | | Sig. (2-tailed) | .053 |
| | | N | 372 |
| | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | Correlation Coefficient | .081 |
| | | Sig. (2-tailed) | .120 |
| | | N | 372 |
| | 16.6. I am not informed about the latest phishing scams (email scams) | Correlation Coefficient | .001 |
| | | Sig. (2-tailed) | .987 |
| | | N | 372 |
| | 16.7. I am not informed about the latest cybersecurity crimes | Correlation Coefficient | -.080 |
| | | Sig. (2-tailed) | .126 |
| | | N | 370 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-57: Correlation of Challenges Towards Students' Compliance vs Access to the University Network Factor 2***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place for the university network. As depicted in Table 4-58 below the regression model significantly predicts the dependent variable outcome (p = 0.014). Student Compliance with Access to the

University Network is represented by one regression model F2= (Constant) + Regression Coefficient =-0.326 - 0.157 * X (where X represents, “I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place”).

| Coefficientsa | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.326 | .177 | | -1.846 | .066 |
| | 16.1. I do not have the required IT skills to comply with UKZN information security measures | -.037 | .069 | -.039 | -.536 | .593 |
| | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | .156 | .063 | .180 | 2.466 | .014 |
| | 16.3. I do not know how to change the password that I use to access the UKZN network | .102 | .057 | .104 | 1.802 | .072 |
| | 16.4. I am not aware of ICS policy with regard to the use of password | .068 | .060 | .077 | 1.149 | .251 |
| | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | -.015 | .063 | -.016 | -.233 | .816 |
| | 16.6. I am not informed about the latest phishing scams (email scams) | .045 | .075 | .055 | .594 | .553 |
| | 16.7. I am not informed about the latest cybersecurity crimes | -.172 | .072 | -.215 | -2.395 | .017 |
| a. Dependent Variable: Q8 Access to the University network f2 | | | | | | |

***Table 4.58: Regression of Challenges Towards Students’ Compliance vs Access to the University Network Factor 2***

A Spearman correlation was performed between the independent construct named Challenges Towards Student Compliance and the 2nd construct from the dependent variable named Student Compliance; the 2nd construct in the dependent variable is named Access to the University Network which will be represented as factor 3 (F3) of the dependent variable; F3 consists of 1 item, the Spearman correlation was performed between Challenges Towards Student Compliance and the single index value generated for F3. The correlation reveals that there is a significant and negative correlation between F3 and students’ perception that they do not have the required IT skills to comply with

UKZN information security controls (rho=-0.121, p=0.020, N=371). The correlation reveals that there is a significant and negative correlation between F3 and students' perception that they are not aware of ICS policy with regard to the use of password (LANs) (rho=-0.178, p=0.001, N=372). The correlation reveals that there is a significant and negative correlation between F3 and students' perceptions that they are not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) (rho=-0.133, p=0.010, N=372). In addition, the correlation reveals that there is a significant and negative correlation between F3 and students' perception that they are not informed about the latest phishing scams (email scams) (rho=-0.152, p=0.003, N=372). Finally, the correlation reveals that there is a significant and negative correlation between F3 and students' perception that they are not informed about the latest cybersecurity crimes (rho=-0.173, p=0.001, N=370) as depicted in Table 4-59 below.

| | | | Q8 Access to the University network f3 |
|---|---|---|---|
| Spearman's rho | Q8 Access to the University network f3 | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 372 |
| | 16.1. I do not have the required IT skills to comply with UKZN information security measures | Correlation Coefficient | -.121* |
| | | Sig. (2-tailed) | .020 |
| | | N | 371 |
| | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | Correlation Coefficient | -.091 |
| | | Sig. (2-tailed) | .079 |
| | | N | 372 |
| | 16.3. I do not know how to change the password that I use to access the UKZN network | Correlation Coefficient | -.022 |
| | | Sig. (2-tailed) | .678 |
| | | N | 371 |
| | 16.4. I am not aware of ICS policy with regard to the use of password | Correlation Coefficient | -.178** |
| | | Sig. (2-tailed) | .001 |
| | | N | 372 |
| | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | Correlation Coefficient | -.133* |
| | | Sig. (2-tailed) | .010 |
| | | N | 372 |
| | 16.6. I am not informed about the latest phishing scams (email scams) | Correlation Coefficient | -.152** |
| | | Sig. (2-tailed) | .003 |
| | | N | 372 |
| | 16.7. I am not informed about the latest cybersecurity crimes | Correlation Coefficient | -.173** |
| | | Sig. (2-tailed) | .001 |
| | | N | 370 |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |

***Table 4-59: Correlation of Challenges Towards Students' Compliance vs Access to the University Network Factor 3***

Furthermore, a linear regression analysis was carried out with the purpose of determining the effect of the variables on compliance with measures put in place for the university network. As depicted in Table 4-60 below the regression model significantly predicts the dependent variable outcome (p = 0.006). Student Compliance with Access to the University Network is represented by one regression model F3= (Constant) + Regression Coefficient =0.549- 0.164* X (where X represents, "I am not aware of ICS policy with regard to the use of password").

| Coefficientsa | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | .549 | .176 | | 3.114 | .002 |
| | 16.1. I do not have the required IT skills to comply with UKZN information security measures | -.111 | .069 | -.118 | -1.625 | .105 |
| | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | .051 | .063 | .059 | .815 | .416 |
| | 16.3. I do not know how to change the password that I use to access the UKZN network | .147 | .057 | .149 | 2.596 | .010 |
| | 16.4. I am not aware of ICS policy with regard to the use of password | -.164 | .059 | -.185 | -2.758 | .006 |
| | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | -.005 | .063 | -.006 | -.084 | .933 |
| | 16.6. I am not informed about the latest phishing scams (email scams) | -.053 | .075 | -.065 | -.702 | .483 |
| | 16.7. I am not informed about the latest cybersecurity crimes | -.048 | .072 | -.060 | -.669 | .504 |
| a. Dependent Variable: Q8 Access to the University network f3 | | | | | | |

***Table 4.60: Regression of Challenges Towards Students' Compliance vs Access to the University Network Factor 3***

### 4.7. Concluding Remarks

Chapter 4 presented the analysis of the responses attained from students and how the data was checked for any missing values. This chapter revealed the procedures taken to test the reliability and validity of the questions within the questionnaire through cronbach alpha and factor analysis tests. Test for normality and descriptive statistical analysis of the data was performed in this chapter. Furthermore, correlation, regression and thematic analysis were conducted in this chapter. This section reports on the findings based on the responses from participants, additional interpretation and discussion are provided in the next chapter, chapter 5

# CHAPTER 5: RESULT DISCUSSION

## 5.1. Introduction

The previous chapter presented the data analysis of the following research questions, how compliant are students with the existing information security measures currently within the university; What are the effects of Threat Appraisal on students' compliance with the information security measures within the university; What are the effects of Coping Appraisal on students' compliance with the information security measures within the university; What are the challenges faced by students in their compliance with the information security measures within the university; This chapter will discuss the findings in relation to the existing literature pertaining student's compliance with the university's information security measures.

## 5.2. Discussion of the findings

### 5.2.1. Research Question 1: How Compliant are Students with the Existing Information Security Measures Currently in Place within the University?

#### 5.2.1.1. Student's Compliance with Physical Access to Computer Rooms

The findings revealed that students are complying with always using their own student cards to access computer facilities. However, most students sometimes do ask other students to give them access to the computer facilities. Therefore, most students do abide by university rules. Furthermore, most students let other students access the computer rooms using their cards. As per the university rules, students are not allowed to let others use their student cards to access or ask other students to give them access to the computer facilities (Information & Communication Services, 2022). Hence, from these responses most students are not abiding by university rules. This is similar to a study conducted by Siponen et al. (2010).

#### 5.2.1.2. Student's Compliance with Access to the University Network

Findings from this research indicate that the majority of students utilise their personal login credentials to access the UKZN network. Thus, complying with the university rules. Furthermore, most students comply with university rules by not using someone else's login details or login credentials to access the university network. Moreover, most students comply with the university rule of not allowing other people to use their login credentials to access the university network. Furthermore, the findings of this research

show that most students are not complying with the university rule, which states that students must always change their password at least every three months. However, the findings also reveal that the majority of the students always use a strong password to access the university network as recommended by the UKZN ICS department. Thus, complying with the university rules that students must always change their password at least once in 3 months (Information & Communication Services, 2022). Furthermore, most students comply with the university rule regarding not revealing the password they use to access the UKZN network to anyone else. Moreover, most students do not provide their UKZN login details when requested via email. Furthermore, most students take information security precautionary measures as advised through the UKZN email alerts. Thus, complying with the university rules in place. Additionally, most students have not been victims of phishing scams while using the UKZN network.

These results confirm the previous study conducted by Kim (2013) that students do not frequently change their passwords. Moreover, Kim (2013); McCrohan et al. (2010) Wash et al. (2016) study support the findings of this study that students always use a strong password and do not provide it via email. However, Tanni et al. (2022), conducted a study which revealed that students use weak passwords. Wash et al. (2016) found that university students do share their passwords with other people. This is in contrast with the results obtained in this study. A study conducted by Kim (2013) at a business college corroborates the findings of this study that student claimed that they were never victims of phishing.

#### 5.2.1.3. Awareness of UKZN Information Systems Policies

Students who participated in this study indicated that they are aware of UKZN policies regarding physical access to computer rooms and they also indicated that they are aware of UKZN policies regarding access to the UKZN network. Thus, complying with the university rules, which state that students should familiarize themselves with UKZN policies concerning physical and network access Fields(Information & Communication Services, 2022). In addition, most students are complying with the university rule which states that students must be aware of UKZN policies regarding choosing a strong password (Information & Communication Services, 2022). However, more than half of the students are noncompliant towards checking the ICS website regularly to acquaint themselves with new information security alerts.

Foltz and Hauser (2005); Yildirim and Mackie (2019) discovered that students are aware of their institution's policies and guidelines, this is similar to what was found in this study. Tanni et al. (2022) carried out a study on the topic of creating secure passwords, and the results indicated that students lack knowledge on how to create a strong password. This contradicts the findings from this study.

#### 5.2.1.4. Reasons for not Complying with Information Security Measures

The results obtained from this study suggest that most students do not comply due to a lack of knowledge and understanding concerning information security. Moreover, some of the respondents stated that they do not have enough time to educate themselves on data security. Furthermore, students stated that they are lazy to read these information security policies and security measures. Moreover, some students stressed that the existing student card system causes them not to comply because they forget their student cards and need someone to give them access and vice versa. In addition, the study revealed that students the lack of attention to the email warning about threats from the UKZN's Information & Communication Services (2018) department.

According to Gundu and Flowerday (2013) worker in small and medium enterprise (SME) engineering company lack knowledge and skills concerning information security this in alignment with this study which found students do not comply because they lack knowledge. This is confirmed by Gundu and Flowerday (2013) after conducting a similar study lack and obtaining result that suggest students lack knowledge and understanding concerning information security.

### 5.2.2. Research Question 2: What are the Effects of Threat Appraisal on Students' Compliance with the Information Security Measures within the University?

#### 5.2.2.1. Influence of Perceived Vulnerability on Students' Compliance with Information Security Measures in Place

The results of this study reveal that most students agree that they can be victims of a severe data security threat and that UKZN can be susceptible to a severe data security threat. Vance et al. (2012) conducted a similar study and found similar results. Moreover, most students do not agree or disagree that UKZN faces a growing number of serious data security threats. As of March 2018, the Information & Communication Services (2022) department announced to all students of the university that it is currently facing more and

more security attacks due to weak passwords, and this indicates that students are not aware of the latest news concerning the information security attacks of the university. Furthermore, this proves that students do not regularly visit the ICS website (or ICS emails) to acquaint themselves with the latest policies and measures to protect themselves from cyber-attacks.

A Spearman correlation and linear regression analysis were performed between Perceived Vulnerability and factor 1 of Student Compliance with Physical Access to Computer Rooms construct. A positively significant correlation was found between question 10.1 ("I could be a victim of a serious information security threat") and question 10.2 ("UKZN could be subjected to a serious information security threat") with Student Compliance with Physical Access to Computer Rooms. This suggests that students who perceive themselves or the university to be at a higher risk of a serious information security threat are more likely to comply with UKZN policies regarding physical access to computer rooms. Furthermore, the regression model significantly predicts the outcome of Student Compliance with Physical Access to Computer Rooms.

A Spearman correlation was performed between Perceived Vulnerability and factor 1 and factor 3 of Student Compliance with Access to the University Network construct. No significant correlation was found between Perceived Vulnerability and Student Compliance with Access to the University Network factors 1 and 3. However, a Spearman correlation and linear regression analysis were performed between Perceived Vulnerability and factor 2 of Student Compliance with Access to the University Network construct. A positively significant correlation was found between question 10.1 ("I could be a victim of a serious information security threat"), question 10.2 ("UKZN could be subjected to a serious information security threat"), and question 10.3 ("UKZN faces a growing number of serious data security threat") with Student Compliance with Access to the University Network. This suggests that students who perceive themselves or the university to be at a higher risk of a serious information security threat are more likely to comply with UKZN policies regarding access to the university network. In addition, the finding suggests that students who perceive the University (UKZN) as facing a growing number of serious data security threats may be more likely to comply with UKZN policies regarding access to the university network. Moreover, the finding of this study revealed

that the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

Vance et al. (2012) also conducted a similar study and found that Perceived Vulnerability has less influence on compliance. McCrohan et al. (2010)'s study revealed that students believed that the institution and themselves could be subjected to information security threats. Workman et al. (2008) stated that Perceived Vulnerability could be utilised to explain the probability of users forgetting security precautions. Vance et al. (2012) adding that Perceived Vulnerability does not increase a person's intent to comply. However, their respondents believed they would not be victims of a security threat. Hence, they did not comply measures put in place.

In conclusion, this study has found a positive significant correlation between Perceived Vulnerability and both Student Compliance constructs namely, Physical Access to Computer Rooms (factor 1) and Access to the University Network (factor 2) constructs.

#### 5.2.2.2. Influence of Perceived Severity on Students' Compliance with Information Security Measures in Place

This study revealed that most students believe that a data security breach at UKZN will pose a significant issue for them. Furthermore, the study also revealed that most students believe that they will lose important data if someone steals their login credentials. Moreover, most students agreed that it would be a huge invasion of their privacy if someone stole their login credentials. Moreover, most students believe that they will be in serious trouble if someone accessed the computer rooms using their student card. In addition, the results obtained in this study reveals that most students agree that they will be in serious trouble if someone uses their login details to commit cybercrimes using the university network.

A Spearman correlation and linear regression analysis were performed between Perceived Severity and factor 1 of Student Compliance with Physical Access to Computer Rooms construct. A positive and significant correlation was found for question 11.1 ("An information security breach at UKZN will be a serious problem for me") and compliance with physical access (Factor 1). The finding suggests that students who perceive an information security breach at UKZN as a serious problem for them may be more likely to comply with UKZN policies regarding physical access to computer rooms.

Furthermore, the regression model significantly predicts the outcome of Student Compliance with Physical Access to Computer Rooms.

Moreover, a correlation and regression analysis were run between Perceived Severity and factor 1, 2, and 3 of Student Compliance with Access to the University Network construct. A negatively significant correlation was found between questions 11.2 ("I will lose vital information if my login credential are stolen"), 11.3 ("My privacy will be seriously violated if my login credentials are stolen") and 11.5 ("I will be in serious trouble if someone uses my login details to commit cybercrimes using the university network") and Student Compliance with Access to the University Network (Factor 1). The finding suggests that students who perceive that they are at risk of losing vital information, having their privacy violated, or being in serious trouble if someone uses their login details to commit cybercrimes using the university network, may be less likely to comply with UKZN policies regarding access to the university network. Moreover, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

Furthermore, a positive and significant correlation was found between question 11.2 ("I will lose vital information if my login credential are stolen ") and question 11.4 ("I will be in serious trouble if someone accesses the computer rooms using my student card") and Student Compliance with Access to the University Network (Factor 2). In addition, negative and significant correlation was found between question 11.5 ("I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network") and Student Compliance with Access to the University Network (Factor 2).

This suggests that individuals who perceive that they are at risk of losing vital information or being in serious trouble if someone access the computer rooms using their student card are more likely to comply with UKZN policies regarding access to the university network. Additionally, the study found a negative and significant correlation between Perceived Severity of potential risks associated with access to the university network. This suggests that individuals who perceive that they are at risk of being in serious trouble if someone uses their login details to commit cybercrimes using the University network are less likely to comply with UKZN policies regarding access to the university network. Furthermore, the two regression models significantly predict the outcome of Student Compliance with Access to the University Network.

Moreover, a positively significant correlation was found between question 11.2 (“I will lose vital information if my login credential are stolen “), question 11.3 (“My privacy will be seriously violated if my login credentials are stolen”), and question 11.4 (“I will be in serious trouble if someone access the computer rooms using my student card”) with Student Compliance with Access to the University Network (Factor 3). Moreover, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

This suggests that as Perceived Severity increases, Student Compliance with Access to the University Network also increases. This finding is consistent with studies from Ifinedo (2012); Prasetyo et al. (2020) that found a positive correlation between Perceived Severity and compliance with security measures. The authors found that Perceived Severity was positively associated with behavioural control, which in turn was positively associated with the acceptance of information security policies (Ifinedo, 2012; Prasetyo et al., 2020). The results of this study are also in line with a study conducted by Ghazvini and Shukur (2017), the authors believe that if students knew the consequences of any security breaches that would lead to compliance. Pahnila et al. (2007) conducted a similar study and found that students believe they will be punished if they do not follow policies, which is in alignment with this study.

#### 5.2.2.3. Influence of Perceived Rewards on Students’ Compliance with Information Security Measures in Place

The findings of this research suggest that most students would not feel rewarded if a friend used their student card to access the LAN. Moreover, they would not feel rewarded if friends used their LAN credentials to access the university network. In addition, most students would not benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures.

Moreover, a correlation and regression analysis were run between Perceived Rewards and factor 1 of Student Compliance with Physical Access to Computer Rooms. Factor 1 revealed a positively significant correlation for question 12.1. (“I would feel rewarded if a friend used my student card to access the LAN”), question 12.2 (“I would feel rewarded if a friend used my LAN credentials to access the university network”), and question 12.3 (“I would benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them”). This

suggests that students who perceive that they would feel rewarded if their friend used their student card or LAN credentials to access the university network, or that they would benefit from not complying with security measures are more likely to comply with UKZN policies regarding physical access to computer rooms. Moreover, the regression model significantly predicts the outcome of Student Compliance with Physical Access to Computer Rooms.

A Spearman correlation and linear regression analysis were performed between Perceived Rewards and factors 1, 2, and 3 of Student Compliance with Access to the University Network construct. Factor 1 revealed a positively significant correlation for question 12.1. "I would feel rewarded if a friend used my student card to access the LAN"), question 12.2 ("I would feel rewarded if a friend used my LAN credentials to access the university network"), and question 12.3 ("I would benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them"). This suggests that as students perceive more rewards in sharing their student cards, sharing login credentials or not complying with the university's security measures, they are more likely to comply with UKZN policies regarding access to the university network. Moreover, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

However, factor 2 revealed a negatively significant correlation for question 12.1 ("I would feel rewarded if a friend used my student card to access the LAN"), question 12.2 ("I would feel rewarded if a friend used my LAN credentials to access the university network"), and question 12.3 ("I would benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them"). This suggests that students who believe they would benefit from non-compliance with the university security measures, such as sharing a student card, login credentials or other non-compliances acts such as watching movies online, those students are less likely to comply with UKZN policies regarding access to the university network. Moreover, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

Factor 3 showed a negatively significant correlation between question 12.1 ("I would feel rewarded if a friend used my student card to access the LAN") and question 12.2 ("I would feel rewarded if a friend used my LAN credentials to access the university

network") with Student Compliance with Access to the University Network (Factor 3). This suggests that students who believe they would benefit from non-compliance with the university security measures, such as sharing a student card or login credentials, those students are less likely to comply with UKZN policies regarding access to the university network. However, the regression model does not significantly predict the outcome of Student Compliance with Access to the University Network.

Results obtained from this study are in line with results from a study conducted by Vance et al. (2012), the authors state that Perceived Rewards have a negative influence on compliance. Also, Pahnila et al. (2007) state rewards does not have a significance if no tangible reward is available. This finding is consistent with previous research on how Perceived Rewards and Costs can influence compliance with security policies (e.g. Wang, et al., 2017; Gao, et al., 2016).

This also highlights the need for universities to develop strategies that align students' perceptions of rewards with compliance with security measures. As such, universities should consider ways to make compliance with security measures more rewarding for students, for example by highlighting the benefits (incentives) of complying with UKZN security measures. Additionally, universities should also consider ways to make non-compliance less appealing to students by increasing the risks and consequences associated with non-compliance.

### 5.2.3. Research Question 3: What are the Effects of Coping Appraisal on Students' Compliance with the Information Security Measures within the University?

#### 5.2.3.1. Influence of Response Efficacy on Students' Compliance with Information Security Measures in Place

Results from this study indicate that students believe that complying with UKZN information security measures keeps information systems security breaches down. Furthermore, most students believe that if they comply with information security policies, information systems security breaches will be scarce. In addition, most students also believe that careful compliance with IS security policies helps to avoid IS security problems

A Spearman correlation and linear regression analysis were performed between Response Efficacy and factor 1 of Student Compliance with Physical Access to Computer Rooms

construct. Factor 1 revealed a negative and significant correlation between question 13.1 (“I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft”) and question 13.2 (“I believe that NOT sharing my student card helps to reduce security breaches ”) and Student Compliance with Physical Access to Computer Rooms construct. The negative correlation found in this study indicates that as students' belief in the effectiveness of not sharing their LAN login details in preventing identity theft increases, their compliance with UKZN policies regarding physical access to computer rooms is likely to decrease. Moreover, the finding suggests that as students' belief in the effectiveness of not sharing their student card in mitigating security breaches, their compliance with UKZN policies regarding physical access to computer rooms is likely to decrease. Moreover, the regression model significantly predicts the outcome of Student Compliance with Physical Access to Computer Rooms.

A Spearman correlation and linear regression analysis were performed between Response Efficacy and factor 1, 2 and 3 of Student Compliance with Access to the University Network construct. Factor 1 revealed a negatively significant correlation between question 13.1 (“I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft”) and question 13.2 (“If I comply with information security policies, Information Systems security breaches will be scarce”) and question 13.3 (“If I comply with information security policies, Information Systems security breaches will be scarce”) and Student Compliance with Access to the University Network construct.

This finding suggests that as students perceive a stronger belief in the effectiveness of not sharing their LAN login details in preventing identity theft, there is a corresponding decrease in their compliance with UKZN policies regarding access to the university network. Similarly, the finding also suggests that as students perceive a stronger belief in the effectiveness of not sharing their student card in reducing security breaches, there is a corresponding decrease in their compliance with UKZN policies regarding access to the university network. Additionally, the finding suggests that as students' belief in the effectiveness of complying with information security policies, their compliance with UKZN policies regarding physical access to computer rooms is likely to decrease. Furthermore, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

However, factor 2 revealed no significant correlation between the Response Efficacy construct and factor 2. Factor 3 showed a positive and significant correlation between factor 3 and Response Efficacy in question 13.1 (“I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft”), question 13.2 (“If I comply with information security policies, Information Systems security breaches will be scarce”), and question 13.3 (“If I comply with information security policies, Information Systems security breaches will be scarce”). This finding suggests that as students perceive a stronger belief in the effectiveness of not sharing their LAN login details in preventing identity theft, there is a corresponding increase in their compliance with UKZN policies regarding access to the university network. Similarly, the finding also suggests that as students perceive a stronger belief in the effectiveness of not sharing their student card in reducing security breaches, there is a corresponding increase in their compliance with UKZN policies regarding access to the university network. Additionally, the finding suggests that as students' belief in the effectiveness of complying with information security policies, their compliance with UKZN policies regarding physical access to computer rooms is likely to increase. However, the regression model did not significantly predict the outcome of Student Compliance with Access to the University Network.

According to Tsai et al. (2016), students believe that complying with information security measures keeps information systems security breaches down; this is in alignment with the results of factor 3 of this study. In addition, results attained by Vance et al. (2012) indicate that students believe that careful compliance with policies helps to avoid security problems. Thus, supporting the results of this study. However, Siponen et al. (2014) conducted a similar study, their results are in contrast with the findings of this study. Later adding, Response Efficacy does not significantly impact compliance. Although, Vance et al. (2012) stated that Response Efficacy is positively correlated with intention to comply. Tsai et al. (2016)’s results indicate that Response Efficacy significantly predicts security intentions to comply.

This finding aligns with recent research on the relationship between Response Efficacy and security behaviour. A study by (Carroll, 2013) found that individuals with a higher perceived Response Efficacy were more likely to engage in risky behaviour online, as they believed they had the ability to effectively handle any potential negative consequences. Similarly, a study by McLaughlin and Osborne (2018) found that

individuals with a high Response Efficacy were less likely to comply with information security policies, as they believed they could handle security threats on their own.

The findings of this study highlight the importance of ensuring that students understand the potential risks associated with sharing login details and the ways in which compliance with information security policies can help to prevent or reduce those risks. This highlights the importance of not only implementing security measures, but also effectively communicating their effectiveness to users in order to promote compliance. Additionally, the findings suggest that universities should focus on educating students about the potential consequences of non-compliance and the ways in which compliance can lead to increased security.

#### 5.2.3.2. Influence of Self-efficacy on Students' Compliance with Information Security Measures in Place

The results of this study revealed that many students could comply with UKZN information security measures by themselves. However, most students do not need assistance to comply with UKZN information security measures. In addition, most students are confident enough to comply with UKZN information security measures. Hence, responses from this study indicate that students possess the knowledge and confidence to comply with security measures.

A correlation was run and revealed no significant correlation between the Self-efficacy construct and Physical Access to the Computer Rooms construct(factor 1).

Moreover, a Spearman correlation and linear regression analysis were performed between Self-efficacy and factor 1 of Student Compliance with Access to the University Network construct. Factor 1 revealed a negatively significant correlation for question 14.1 ("I can comply with UKZN information security measures by myself") and a positive significant correlation for question 14.2 ("I need assistance to comply with UKZN information security measures") and question 14.3 ("I am not confident enough to comply with UKZN information security measures"). The finding of a negatively significant correlation between Self-efficacy and Student Compliance with Access to the University Network construct suggests that students who have higher levels of Self-efficacy, or belief in their ability to comply with information security measures, may be less likely to comply with the measures put in place by the university. However, the finding of a positive correlation

suggests that students who acknowledge that they lack confidence and need assistance to comply with the university's information security measures are more likely to comply with them. Furthermore, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

A Spearman correlation and linear regression analysis were performed between Self-efficacy and factor 2 of Student Compliance with Access to the University Network construct. Factor 2 revealed a positive and significant correlation for question 14.2 (“I need assistance to comply with UKZN information security measures”). The findings reveal a positive correlation that suggests that students who acknowledge that they need assistance to comply with the university's information security measures are more likely to comply with them. Moreover, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

Factor 3 revealed a positive and significant correlation for question 14. 1 (“I can comply with UKZN information security measures by myself”). The findings reveal a positive correlation between Self-efficacy and Student Compliance with Access to the University Network construct suggests that students who have higher levels of Self-efficacy, or belief in their ability to comply with information security measures, are more likely to comply with the measures put in place by the university. Moreover, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

The results of this study are in alignment with Vance et al. (2012) results from a similar study that students can comply with information security measures by themselves. Kim (2013) conducted a similar study and found that some students need assistance with information security measures. According to Tsai et al. (2016), students are still not confident enough to comply with information security measures, this is in alignment with the results obtained in this study. Kim (2013); Siponen et al. (2014) conducted a similar study and stated that Self-efficacy is significantly correlated with complying with an organisation’s security measures and policies.

This highlights the importance of addressing Self-efficacy in the development of information security policies to ensure that students are more likely to comply with such measures.

#### 5.2.3.3. Influence of Response Cost on Students' Compliance with Information Security Measures in Place

The responses from this study indicate that most students disagree that complying with information security measures is an inconvenience to them. Moreover, most students indicated that complying with information security measures is not time-consuming. In addition, responses revealed that most students indicated that complying with information security measures does not require a lot of effort other than time.

A correlation was run and revealed no significant correlation between the Response Cost construct and Student Compliance with Physical Access to Computer Rooms construct (factor 1).

However, a Spearman correlation and linear regression analysis were performed between Response Cost and factors 1, 2 and 3 of Student Compliance with Access to the University Network construct. The results revealed that factor 1 had a positively significant correlation for questions 15.1 ("Complying with information security measures is an inconvenience to me"), 15.2 ("Complying with information security measures is time-consuming") and 15.3 ("Complying with information security measures requires a lot of effort other than time"). The findings of a positive significant correlation between Response Cost and factor 1 of Student Compliance with Access to the University Network construct suggests that as Response Cost (i.e. the inconvenience, time consumption and effort required to comply with information security measures) increases, Student Compliance with Access to the University Network is likely to increase. Moreover, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

Moreover, factor 2 revealed a positively significant correlation for questions 15.2 ("Complying with information security measures is time-consuming") and 15.3 ("Complying with information security measures requires a lot of effort other than time"). The finding from this study suggests that as the perception of Response Cost (i.e. the time and effort required to comply with information security measures) increases, there is a positive correlation with factor 2 of Student Compliance with Access to the University Network construct. This implies that students are more likely to comply with information security measures regardless of the time and effort required.

However, factor 3 showed a negatively significant correlation for questions 15.1 ("Complying with information security measures is an inconvenience to me"), 15.2 ("Complying with information security measures is time-consuming") and 15.3 ("Complying with information security measures requires a lot of effort other than time"). The findings of a negative significant correlation between Response Cost and factor 3 of Student Compliance with Access to the University Network construct suggest that as Response Cost (i.e. the inconvenience, time consumption and effort required to comply with information security measures) increases, Student Compliance with Access to the University Network is likely to decrease. In addition, in factors 2 and 3 the regression models did not significantly predict the outcome of Student Compliance with Access to the University Network.

According to Tsai et al. (2016), students believe complying with information security measures is not an inconvenience to them, this is in alignment with the results of this study. However, Vance et al. (2012) conducted a similar study and the results are in contrast with the findings in this research. Moreover, LaRose et al. (2007); Tsai et al. (2016) claimed that coping appraisal significantly predicts security intentions to comply.

In summary, the findings revealed no significant correlation between the Response Cost construct and Student Compliance with Physical Access to Computer Rooms construct. However, the correlation between Response Cost and factor 1 and factor 2 of Student Compliance with Access to the University Network construct. Conversely, the correlation between Response Cost and factor 3 revealed a negative significant correlation. Therefore, reducing the perceived inconvenience of complying with information security measures may be an effective strategy for increasing compliance among university students.

### 5.2.4. Research Question 4: What are the Challenges Faced by Students in their Compliance with the Information Security Measures within the University?

The findings from this research indicate that most students have the required IT skills to comply with UKZN information security measures. Furthermore, most students have enough cybersecurity knowledge to comply with UKZN information security measures in place. Moreover, most students know how to change the password that they use to access the UKZN network. Furthermore, more than half of the students are aware of ICS

policy regarding the use of passwords. In addition, most students are aware of ICS/UKZN policy regarding accessing computer rooms. Furthermore, more than half of the students claim that they are informed about the latest phishing scams. In addition, most students claim that there are informed about the latest cybersecurity crimes.

A Spearman correlation and linear regression analysis were performed between challenges faced by students and factor 1 of Student Compliance with Physical Access to Computer Rooms. Factor 1 showed a significant and positive correlation with questions 16.2 ("I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place"), 16.3 ("I do not know how to change the password that I use to access the UKZN network"), 16.4 ("I am not aware of ICS policy with regard to the use of password"), and 16.5 ("I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs)"). This implies that students are more likely to comply with UKZN security measures pertaining to physical access to computer rooms regardless of their challenges such as changing passwords, inadequate cybersecurity knowledge and lack of awareness of ICS/UKZN policies. Moreover, the regression model significantly predicts the outcome of Student Compliance with Physical Access to Computer Rooms.

A Spearman correlation and linear regression analysis were performed between challenges faced by students and factors 1, 2 and 3 of Student Compliance with Access to the University Network. Factor 1 showed a significant and positive correlation with questions 16.3 ("I do not know how to change the password that I use to access the UKZN network"), 16.4 ("I am not aware of ICS policy with regard to the use of password"), 16.5 ("I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs)"), and 16.6 ("I am not informed about the latest phishing scams (email scams)"). This implies that students are more likely to comply with UKZN security measures pertaining to access to the university network regardless of facing challenges such as changing passwords, lack of awareness of ICS/UKZN policies and not being informed about the latest phishing scams. Furthermore, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

Factor 2 revealed a significant and positive correlation with questions 16.1 ("I do not have the required IT skills to comply with UKZN information security measures") 16.2 ("I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place"), and 16.3 ("I do not know how to change the password that I use to

access the UKZN network"). This implies that students are more likely to comply with UKZN security measures pertaining to access to the university network regardless of facing challenges such as changing passwords, lack of IT skills to comply with UKZN measures, and insufficient cybersecurity knowledge. Additionally, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

These results are in alignment with the results obtained from previous research conducted by Kim (2013); McCrohan et al. (2010) that students are aware of policies with regard to passwords and that they are able to change them themselves.

Factor 3 revealed a significant and negative correlation with questions 16.1 ("I do not have the required IT skills to comply with UKZN information security measures"), 16.4 ("I am not aware of ICS policy with regard to the use of password"), 16.4 ("I am not aware of ICS policy with regard to the use of password"), 16.5 ("I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs)"), 16.6 ("I am not informed about the latest phishing scams (email scams)"), and 16.7 ("I am not informed about the latest cybersecurity crimes"). This implies that students who face challenges such as a lack of IT skills to comply with UKZN security measures, a lack of awareness of ICS/UKZN policies and not being informed about the latest phishing scams and cybercrimes tend to have a lower level of compliance with UKZN security measures pertaining to access to the university network. In addition, the regression model significantly predicts the outcome of Student Compliance with Access to the University Network.

These findings suggest that educational interventions aimed at increasing students' knowledge and awareness of information security measures may be effective in increasing compliance with physical access measures to computer rooms. These studies have also found that providing training and education on information security can help increase compliance among students.

### 5.3. Concluding Remarks

This chapter discussed the findings from chapter 4, the findings ultimately revealed that Perceived Severity and Perceived Rewards exert the strongest influence on students' compliance with information security measures. Moreover, the following chapter concludes this study and provides recommendations based on the above discussion.

# CHAPTER 6: CONCLUSION AND RECOMMENDATION

## 6.1 Introduction

This chapter concludes the entire study. This chapter further provides recommendations based on findings and discussion provided in the previous chapters

## 6.2. Conclusion of the study

This chapter introduced the information security concept, addressed the gap and the background of this study, outlined the significance and justification for conducting this study. This chapter also introduced the research problem, question, objectives, methodology and limitations the study faced.

Chapter 2 provided a literature review pertaining to compliance with information security systems. This chapter discussed the human factor associated with information security compliance, measures and controls that minimize security breaches, the type of policies that exist and should be enforced by institutions, methods of improving information security compliance culture, and the protection motivation theory of this study.

Chapter 3 presented the research design and approach used in this study. Moreover, it presents the study site, target population, sampling process, sample size, sampling strategies, data collection methods, quality control, and data analysis used in this study. Also, the ethics upheld in the study.

Chapter 4 chapter presents the analysis of the responses attained from students. It reveals the procedures taken to test the reliability and validity of the questions within the questionnaire and how the data was checked for any missing values. A descriptive statistical analysis of the data is performed in this chapter. This chapter only reports the results as obtained from the respondents, further interpretations and discussion of the results are presented in chapter 5.

Chapter 5 discusses the findings in relation to the existing literature and research questions of the study. Furthermore, chapter 5 discusses the extent to which students comply with existing information systems security measures put in place by the institution. Research Question 1(RQ1) revealed that students use their own student cards to access computer facilities. However, they sometimes grant each other access to computer facilities. RQ1 also revealed that students utilise their own login credentials to access the UKZN network. Moreover, students indicated that they do not borrow or let

anyone else use their login credentials and they use a strong password. In addition, students indicated that they do not provide their UKZN login details when requested via email and they take information security precautionary measures as advised through the UKZN email alerts. However, students indicated that they do not change their password at least every three months.

RQ1 showed that students are aware of UKZN policies regarding physical access to computer rooms and access to the UKZN network. Moreover, most students are of policies regarding choosing a strong password. However, more than half of the students do not visit the ICS website regularly to acquaint themselves with new information security policies. RQ1 revealed that a significant portion of students is non-compliant due to a lack of knowledge and understanding regarding information security. Moreover, some students stated that a lack of time and laziness hinders their efforts to educate themselves on information security.

Chapter 5 also discussed the influence of Threat Appraisal on student compliance with information security measures. In Research Question 2(RQ2), Perceived Vulnerability revealed a positive significant correlation against Student Compliance with Physical Access to Computer Rooms constructs. However, F1 and F3 of Student Compliance with Access to the University Network construct revealed no significant correlation against Perceived Vulnerability. Nevertheless, F2 revealed a positive significant correlation against Perceived Vulnerability.

Perceived Severity revealed a positive significant correlation against Student Compliance with Physical Access to Computer Rooms constructs. Conversely, F1 of Student Compliance with Access to the University Network construct revealed a negative significant correlation against Perceived Severity. However, F2 revealed a positive and a negative significant correlation against Perceived Severity. Whereas F3 revealed a positive significant correlation against Perceived Severity

Perceived Rewards revealed a positive significant correlation against Student Compliance with Physical Access to Computer Rooms constructs. Similarly, F1 of Student Compliance with Access to the University Network construct revealed a positive significant correlation against Perceived Rewards. However, F2 and F3 revealed a positive significant correlation against Perceived Rewards.

Chapter 5 also discussed the influence of Coping Appraisal on student compliance with information security measures. In Research Question 3(RQ3), Response Efficacy revealed a negative significant correlation against Student Compliance with Physical Access to Computer Rooms constructs. Similarly, F1 of Student Compliance with Access to the University Network construct revealed a negative significant correlation against Response Efficacy. However, F2 and F3 revealed no significant correlation against Response Efficacy.

Self-efficacy revealed no significant correlation against Student Compliance with Physical Access to Computer Rooms constructs. However, F1 of Student Compliance with Access to the University Network construct revealed a positive and negative significant correlation against Self-efficacy. Whereas F2 and F3 revealed a positive significant correlation against Self-efficacy.

Response Cost revealed no significant correlation against Student Compliance with Physical Access to Computer Rooms constructs. However, F1 and F2 of Student Compliance with Access to the University Network construct revealed a positive significant correlation against Response Cost. Conversely, F3 revealed a negative significance against Response Cost. Finally, the findings ultimately revealed that Perceived Severity and Perceived Rewards exert the strongest influence on students' compliance with information security measures.

In addition, Chapter 5 revealed that students who face challenges such as a lack of IT skills to comply with UKZN security measures, a lack of awareness of ICS/UKZN policies and not being informed about the latest phishing scams and cybercrimes tend to have a lower level of compliance with UKZN security measures pertaining to access to the university network.

### 6.3. Recommendations for Academic Institutions

Based on the study above, RQ1 revealed that most students sometimes ask other students to give them access to the computer facilities and most students sometimes let other students access the computer rooms using their cards. Hence, RQ1 revealed that most do not comply with UKZN security rules and policies regarding physical access to computer rooms. This study recommends that the UKZN and other institutions change their physical access to the university and computer rooms, this study revealed that the student card system is one of the leading causes of non-compliance because they always forget

them. An innovative and simple method to access the university is utilizing biometric fingerprint scanners. This would ensure that students comply with physical access security measures. However, if the previous suggestion is not feasible, this study suggests that the current student card system be altered to only allow access to one student at a designated time interval, such as ten-minute intervals. This would prevent students from sharing access with multiple students during that time period.

RQ1 also revealed that more than half of the students in this study are non-compliant towards checking the ICS website regularly to acquaint themselves with new information security alerts. This study recommends ICS department to implement a new form of communication to inform students about the latest policies and security measures because students are not reading the announcements through the website and emails, such as SMS (Short Message Service) system to supplement on the email communication system. Moreover, the UKZN ICS department and other institutions are advised to ensure that information security policies are written in a brief, concise and understandable language. A good method to confirm this is to let various departments evaluate the policies for readability prior to implementation.

RQ2 Perceived Rewards correlation against Student Compliance with Access to the University Network (Factor 3) revealed that students respond well to rewards. This study recommends that the UKZN and other institutions to develop strategies that align students' perceptions of rewards with compliance with security measures. Therefore, this study recommends that universities implement methods to make compliance with security measures more rewarding for students, for instance, by emphasizing incentives for adhering to security measures to instil compliance in students. For example, the university can provide free printing credit for students that comply with changing their password at least once in three months.

The correlation between Response Efficacy and Student Compliance in QR3 emphasizes the significance of not only implementing security measures, but also effectively communicating their efficacy to students in order to foster student compliance. Furthermore, the study results imply that UKZN and other institutions should concentrate on educating students about the potential ramifications of non-compliance. Moreover, this study recommends that UKZN and other institutions should also consider ways to make non-compliance less appealing to students by increasing the risks and consequences

associated with non-compliance. Moreover, the findings from this study suggests that UKZN along with other institutions deploy hands-on training workshops for students frequently (every semester). This is because RQ1 and RQ3 also revealed that most students still need assistance with complying with information security measures and some are unaware of cyber-related threats. Moreover, UKZN along with other institutions are advised to develop a game-based delivery method or a video-based delivery method of policies to combat security threats. This is because RQ1 revealed that most students claim that they are lazy to read the policies.

### 6.4. Limitations and Recommendations for future studies

Based on the study's limitations, future studies should aim to conduct research at multiple universities, in order to increase the sample size and diversity of the study and improve the generalizability of the results. As this study was limited to one university (UKZN).

This study was restricted to utilizing only the quantitative method. Future studies should consider utilizing both quantitative and qualitative methods to gain a deeper understanding of the participants' experiences and gain a more comprehensive understanding of the study. Furthermore, the researchers could incorporate interviews with security experts who manage the security infrastructure at the universities to supplement their research. Moreover, future studies should consider incorporating recommendations from security experts and students on how to increase security compliance among students.

In addition, it is important to note that correlation does not imply causality and further research is needed to understand the underlying mechanisms driving the relationship between PMT constructs and student compliance. Moreover, more research is needed to confirm and expand upon these findings. Additionally, it would be interesting to examine if there are any moderating variables that influence the relationship between PMT constructs and non-compliance.

# APPENDICES

## Appendix A – Ethical Clearance

UNIVERSITY OF
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

31 October 2019

Mr Sabelo Moses Masinga (214552237)
School Of Man Info Tech &Gov
Pietermaritzburg Campus

Dear Mr Masinga,

**Protocol reference number**: HSSREC/00000680/2019
**Project title**: Understanding Students' Compliance Behaviour with the Information Security Measures within a South African University

**Full Approval – Expedited Application**

This letter serves to notify you that your application received on 22 October 2019 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL**

**Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.**

This approval is valid for one year from 31 October 2019.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

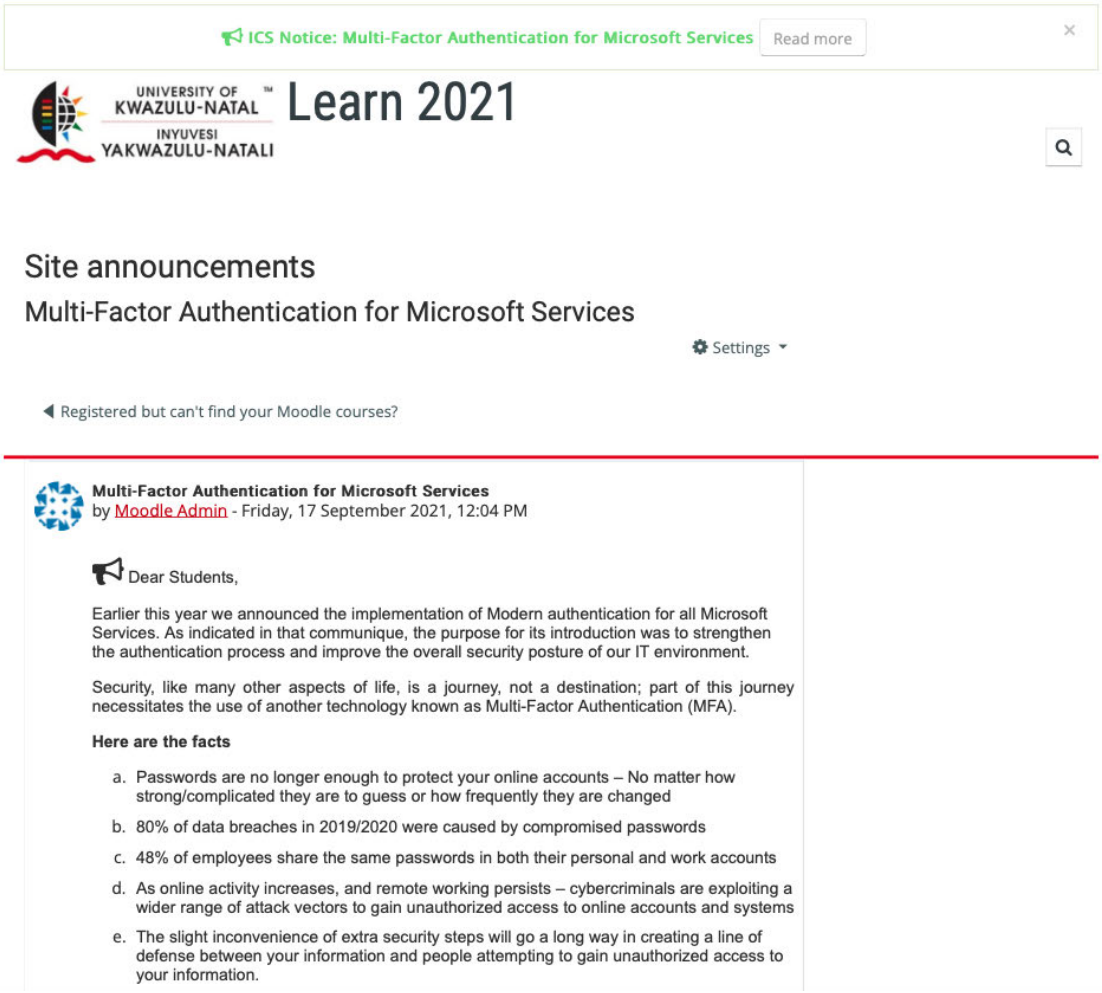
Yours sincerely,

[redacted]

**Professor Urmilla Bob**
**University Dean of Research**

**/dd**

## Appendix B – UKZN Data Breaches



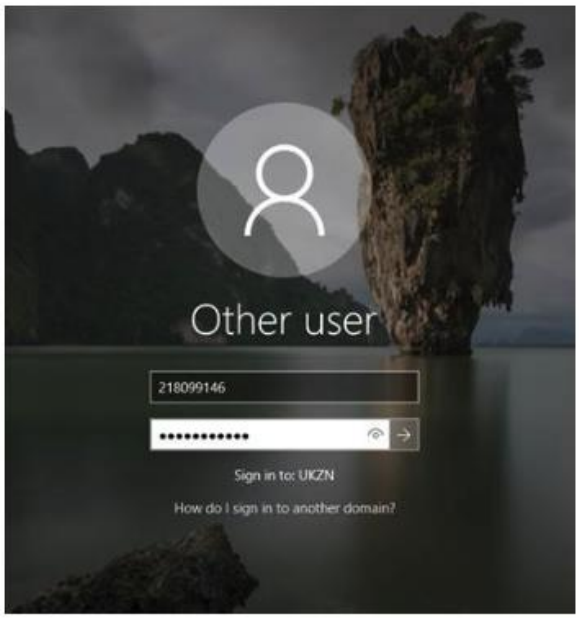
**Monday, January 9, 2023 at 10:49:12 South Africa Standard Time**

**Subject:** ICS Notice: Password Change
**Date:** Friday, 23 March 2018 at 14:41:59 South Africa Standard Time
**From:** University Notice
**To:** University Notice
**Priority:** High
**Attachments:** image001.jpg, image002.jpg, image003.jpg, image004.png

Dear Students,

Due to the recent increase in spam e-mails originating from university e-mail accounts, ICS will be enabling a **mandatory password change** for your University of Kwa-Zulu Natal Active Directory logins.

Your Active Directory login affects your LAN login, email account password, Moodle login, WiFi connection and many other linked systems where you may need to type your login name and password.




Most of these emails are due to compromised email accounts where **weak passwords** have made it easy for an attacker to abuse a valid student or staff email account. Weak passwords can be easily guessed, observed whilst you type or retrieved by skilled attackers using sophisticated software.

Further, these compromised accounts are used to send emails that form part of a phishing campaign directed at acquiring more account names, email addresses, passwords and personal information.

To control this spate of abuse and reduce the incidents of weak passwords a forced password change for everyone has become necessary.

## Appendix C – Questionnaires from Previous Studies

Questionnaire from Burns et al. (2017) below.

| | | | |
|---|---|---|---|
| **Threat severity**[i] (Workman et al., 2008) | Instructions: "Please indicate your level of agreement with the following statements about information security threats to your organization:" | | |
| | TS-1. Threats to the security of my organization's information and information systems are severe. | 3.17 | 1.70 |
| | TS-2. In terms of information security violations, attacks on my organization's information and information systems are severe. | 2.98 | 1.64 |
| | TS-3. I believe that threats to the security of my organization's information and information systems are serious. | 3.81 | 1.85 |
| | TS-4. I believe that threats to the security of my organization's information and information systems are significant. | 3.54 | 1.77 |
| **Security response efficacy**[i] (Workman et al., 2008) | Instructions: "Please indicate your level of agreement with the following statements about yourself and information security threats to your organization:" | | |
| | RE-1. Employee efforts to keep my organization's information and information systems safe from information security threats are effective. | 5.34 | 1.28 |
| | RE-2. The available measures that can be taken by employees to protect my organization's information and information systems from security violations are effective. | 5.37 | 1.32 |
| | RE-3. The preventive measures available to me to stop people from accessing my organization's information and information systems are adequate. | 5.32 | 1.32 |
| | RE-4. If I perform the preventive measures available to me, my organization's information and information systems are less likely to be exposed to a security threat. | 5.43 | 1.46 |
| **Security self-efficacy**[i] (Workman et al., 2008) | Instructions: "Please indicate your level of agreement with the following statements about yourself and the information security threats to your organization:" | | |
| | SSE-1. For me, taking information security precautions to protect my organization's information and information systems is easy. | 5.38 | 1.30 |
| | SSE-2. I have the necessary skills to protect my organization's information and information systems from information security violations. | 5.06 | 1.53 |
| | SSE-3. My skills required to stop information security violations against my organization's information and information systems are adequate. | 5.14 | 1.46 |
| | SSE-4. I believe that I could learn to perform the preventive measures to protect my organization's information and information systems effectively. | 5.43 | 1.40 |
| **Response cost**[i] (Workman et al., 2008) | Instructions: "Please indicate your level of agreement with the following statements about yourself and information security threats to your organization:" | | |
| | RC-1. The inconvenience of implementing recommended security measures to protect my organization's information and information systems exceeds the potential benefits. | 2.89 | 1.68 |
| | RC-2. The negative impact on my work from recommended security measures to protect my organization's information and information systems is greater than the benefits gained from the security measures. | 2.80 | 1.56 |
| | RC-3. Recommended security measures are so much of a nuisance that I think my organization would be better without them. | 2.41 | 1.55 |
| | RC-5. The negative side effects of recommended security measures in my organization are greater than the advantages. | 2.62 | 1.56 |
| **Threat vulnerability**[i] (Workman et al., 2008) | Instructions: "Please indicate your level of agreement with the following statements about information security threats to your organization:" | | |
| | TV-1. My organization's information and information systems are vulnerable to security threats. | 3.34 | 1.65 |
| | TV-2. It is likely that an information security violation will occur to my organization's information and information systems. | 3.36 | 1.68 |
| | TV-3. My organization's information and information systems are at risk to information security threats. | 3.43 | 1.69 |
| | TV-4. My organization's information and information systems are | 3.50 | 1.66 |

Questionnaire from Sommestad et al. (2015) below.

| Construct | Questionnaire Item |
|---|---|
| Protection motivation | I am likely to follow the organization's information systems security policy in the future. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) |
| Rewards | I would feel [a] of sense of internal satisfaction for allowing information security threats to harm my organization. (Strongly agree<->Strongly disagree) (Posey, Roberts, Lowry, Courtney, & Bennett, 2011) |
| Severity | I believe the productivity of [the] organization and its employees is threatened by security incidents. (Strongly agree<->Strongly disagree) (Herath & Rao, 2009) |
| Vulnerability | I know my organization could be vulnerable to security breaches if I don't adhere to its information security policy. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) |
| Response efficacy | Enabling the security measures on my work computer is an effective way to deter hacker attacks. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) |
| Self-efficacy | For me, taking information security precautions to protect my organization's information and information systems is easy. (Strongly agree<->Strongly disagree) (Posey et al., 2011) |
| Response cost | There are too many overhead costs associated with implementing information system security. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) |

Questionnaire from Bakar et al. (2021) below.

| | | | |
|---|---|---|---|
| The inconvenience of implementing recommended security measures to protect my organization's information and information systems exceeds the potential benefits | PC4 | .820 | |
| Backing up data on my computer requires a significant amount of time | PC2 | .802 | |
| Backing up data on my computer requires significant financial cost | PC1 | .677 | |
| The negative side effects of recommended security measures in my organization are greater than the advantages | PC7 | | .921 |
| The negative impact on my work from recommended security measures to protect my organization's information and information systems is greater than the benefits gained from the security measures | PC5 | | .899 |
| It is likely that I would receive personal rewards for purposely not protecting my organization's information and information systems from security threats | MR1 | | .872 |
| Recommended security measures are so much of a nuisance that I think my organization would be better without them | PC6 | | .708 |
| I could be rewarded personally for not protecting my organization from information security threats | MR2 | | .583 |
| I would feel a sense of internal satisfaction for allowing information security threats to harm my organization | MR4 | | .841 |
| I could be rewarded financially for choosing not to protect my organization's information and information systems from security threats | MR5 | | .830 |
| I believe others would be willing to reward me financially for intentionally failing to protect my organization's information and information systems from security threats | MR6 | | .793 |

| | | | | | |
|---|---|---|---|---|---|
| I would receive personal gratification for purposefully not protecting my organization from its information security threats | MR3 | | .759 | | |
| Backing up data on my computer requires significant cognitive effort (brainpower) | PC3 | | | .829 | |
| Eigen Value | | 9.113 | 4.573 | 1.905 | 1.259 |
| % Variance | | 45.563 | 22.867 | 9.526 | 6.297 |
| Cumulative Variance Explained | | 45.563 | 68.430 | 77.956 | 84.253 |

**OF: Organizational Factor, PSV: Perceived Security Vulnerability, PC: Prevention Cost, MR: Maladaptive Reward, F: Fear. Cronbach's Alpha= 1.00 Yellow highlighter indicates factor loading**

## Appendix D – Questionnaire

**Understanding students' compliance behaviour with the information security measures within a South African University**

**ETHICAL CLEARANCE NO: HSSREC/00000680/2019**
**Researcher**: Sabelo Masinga
**Supervisor**: Nurudeen Ajayi

- Please kindly complete this questionnaire.
- Please note that there is no correct/incorrect answer.
- Please note that participation in the study is voluntary.
- Please sign the letter of informed consent, giving me permission to use your responses for this research project.
- Please kindly take note of the instructions before answering any question(s).

**GENERAL INSTRUCTION 1:** In all the sections, kindly provide your response by making a tick (✓) in the appropriate box and fill in the gaps in the case of open-ended questions.

**SECTION A: DEMOGRAPHIC INFORMATION**

| | | | | | |
|---|---|---|---|---|---|
| 1. | **Age:** | ☐ Less than 18 | ☐ 18 - 24 | ☐ 25 - 30 | ☐ 31 and above |
| 2. | **Gender:** | ☐ Female | ☐ Male | | |
| 3. | **Ethnicity:** | ☐ African | ☐ Indian | ☐ Coloured | ☐ White |
| | | Other (please specify): | | | |
| 4. | **Academic level:** | ☐ First year | ☐ Second year | ☐ Third year | ☐ Honors |
| | | ☐ Masters | ☐ PhD | Other (please specify): | |
| 5. | **School:** | ☐ Management, IT and Governance | ☐ Accounting, Economics and Finance | ☐ Law | ☐ Graduate School of Business and Leadership |
| | | Other (please specify): | | | |
| 6. | **Campus:** | ☐ Pietermaritzburg | ☐ Westville | Other (please specify): | |

## SECTION B: INFORMATION ABOUT ACCESS TO COMPUTER ROOMS, UKZN NETWORK AND KNOWLEDGE OF UKZN INFORMATION SYSTEMS SECURITY POLICIES

### TO WHAT EXTENT DO YOU AGREE WITH THE FOLLOWING STATEMENTS?

### 7. Physical access to computer rooms

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 7.1 | I always use my student card to access computer facilities (LANs). | | | | | |
| 7.2 | I sometimes ask students to grant me access to computer facilities (LANs). | | | | | |
| 7.3 | I sometimes let students access the LANs using my student card. | | | | | |

### 8. Access to the University network

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 8.1 | I always use my personal log in details and password to login into the UKZN network. | | | | | |
| 8.2 | I sometimes use someone else login details (username and password) to access the university network. | | | | | |
| 8.3 | I sometimes allow other people to use my login details (username and password) to access the university network | | | | | |
| 8.4 | I always change my password (to access the University network) at least once in 3 months. | | | | | |
| 8.5 | I always use a password with combination of combination of letters, numbers and symbols (@, #, $, %, etc.) to access the University network as recommended by the UKZN ICS department. | | | | | |
| 8.6 | The password that I use to access the UKZN network is unknown to anyone else. | | | | | |
| 8.7 | I provide my UKZN login details when requested via email | | | | | |
| 8.8 | I take information security precautionary measures (e.g. frequently changing password, not sharing login details, not click on unknown email links etc.) as advised through the UKZN email alerts. | | | | | |
| 8.9 | 88I have been a victim of phishing scams (email scams) while using the UKZN network. | | | | | |

### 9. Awareness of UKZN information systems policies

| 9.1 | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 9.2 | I am aware of UKZN policies regarding physical access to computer rooms/ LAN. | | | | | |
| 9.3 | I am aware of UKZN policies regarding access to the UKZN network. | | | | | |
| 9.4 | I am aware of UKZN policies regarding choosing a strong password. | | | | | |
| 9.5 | I do check the ICS website regularly to acquaint myself with new information security alerts. | | | | | |

**SECTION C: DETERMINANTS OF INFORMATION SYSTEMS SECURITY COMPLIANCE**

**TO WHAT EXTENT DO YOU AGREE WITH THE FOLLOWING STATEMENTS?**

### 10. Perceived Vulnerability

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 10.1 | I could be a victim of a serious information security threat. | | | | | |
| 10.2 | UKZN could be subjected to a serious information security threat. | | | | | |
| 10.3 | UKZN faces more and more serious information security threats lately. | | | | | |

### 11. Perceived Severity

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 11.1 | An information security breach at UKZN will be a serious problem for me. | | | | | |
| 11.2 | I will lose vital information if my login credentials are stolen. | | | | | |
| 11.3 | My privacy will be seriously violated if my login credentials are stolen. | | | | | |
| 11.4 | I will be in serious trouble if someone accesses the computer rooms using my student card. | | | | | |
| 11.5 | I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network. | | | | | |

### 12. Perceived rewards

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 12.1 | I would feel rewarded if a friend uses my student card to access the LAN. | | | | | |
| 12.2 | I would feel rewarded if a friend uses my LAN credentials to access the university network. | | | | | |
| 12.3 | I benefit from ***NOT*** complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | | | | | |

### 13. Response Efficacy

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 13.1 | I believe that ***NOT*** sharing my LAN login details prevents or reduces chances of identity theft. | | | | | |
| 13.2 | I believe that ***NOT*** sharing my student card helps to reduce security breaches. | | | | | |
| 13.3 | If I comply with information security policies, Information Systems security breaches will be scarce. | | | | | |

### 14. Self-efficacy

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 14.1 | I can comply with UKZN information security measures by myself. | | | | | |
| 14.2 | I need assistance to comply with UKZN information security measures. | | | | | |
| 14.3 | I am not confident enough to comply with UKZN information security measures. | | | | | |

### 15. Response Cost

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 15.1 | Complying with information security measures is an inconvenience to me. | | | | | |
| 15.2 | Complying with information security measures is time-consuming. | | | | | |
| 15.3 | Complying with information security measures requires a lot of effort other than time. | | | | | |

## SECTION D: CHALLENGES TOWARD INFORMATION SECURITY COMPLIANCE
## TO WHAT EXTENT DO YOU AGREE WITH THE FOLLOWING STATEMENTS?

### 16. Obstacles to information security compliance

| | | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|
| 16.1 | I do not have the required IT skills to comply with UKZN information security measures. | | | | | |
| 16.2 | I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place. | | | | | |
| 16.3 | I do not know how to change the password that I use to access the UKZN network. | | | | | |
| 16.4 | I am not aware of ICS policy with regard to the use of a password. | | | | | |
| 16.5 | I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs). | | | | | |
| 16.6 | I am not informed by the university about the latest phishing scams (email scams). | | | | | |
| 16.7 | I am not informed about the latest cybersecurity crimes. | | | | | |

**17. What are the other factors that prevent your compliance to UKZN information security measures in place?**

_____

_____

_____

_____

**THANK YOU FOR YOUR PARTICPATION**

## Appendix E – Reliability and Validity Tests

### Reliability Test - Cronbach's Alpha Test

| Constructs within the Questionnaire | Number of Items | Cronbach's Alpha (α) | Interpretation |
|---|---|---|---|
| Physical access to computer rooms | 3 | .389 | Close to adequate internal consistency |
| Access to the University network | 9 | .360 | Close to adequate internal consistency |
| Awareness of UKZN information systems policies | 4 | .777 | High internal consistency |
| Perceived Vulnerability | 3 | .700 | High internal consistency |
| Perceived Severity | 5 | .720 | High internal consistency |
| Perceived rewards | 3 | .728 | High internal consistency |
| Response Efficacy | 3 | .823 | Very high internal consistency |
| Self-efficacy | 3,2 | .125 | low internal consistency |
| Response Cost | 3 | .837 | Very high internal consistency |
| Challenges to information security compliance | 7 | .807 | Very high internal consistency |
| **Overall** | **43** | **.704** | **High internal consistency** |

### Construct validity test

Physical access to computer rooms

| KMO and Bartlett's Test | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .581 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 332.905 |
| | df | 36 |
| | Sig. | .000 |

| Component Matrix[a] | |
|---|---|
| | Component |
| | 1 |
| 7.2. I sometimes ask students to grant me access to computer facilities (LANs) | .864 |
| 7.3. I sometimes let students access the LANs using my student card. | .849 |
| 7.1. I always use my student card to access computer facilities (LANs) | -.313 |
| Extracted by Principal Component Analysis. | |

## Access to the University network

| KMO and Bartlett's Test | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .581 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 332.905 |
| | df | 36 |
| | Sig. | .000 |

| Component Matrix[a] | | | |
|---|---|---|---|
| | Component | | |
| | 1 | 2 | 3 |
| 8.3. I sometimes allow other people to use my login details (username and password) to access the university network | -.770 | | |
| 8.2. I sometimes use someone else login details (username and password) to access the university network | -.746 | | .333 |
| 8.6. The password that I use to access the UKZN network is unknown to anyone else. | .476 | | .419 |
| 8.1. I always use my personal login details and password to login into UKZN network | .464 | | -.322 |
| 8.4. I always change my password (to access the University network) at least once in 3 months | | .685 | |
| 8.7. I provide my UKZN login details when requested via email | | .610 | |
| 8.9. I have been a victim of phishing scams (email scams) while using the UKZN network | | .562 | -.493 |
| 8.8. I take information security precautionary measures (e.g. frequently changing password, not sharing login details, not click on unknown email links etc.) as advised through the UKZN email alerts. | .454 | .484 | |
| 8.5.I always use a password with a combination of letters, numbers and symbols (@, #, $, %, etc.) to access the University network as recommended by the UKZN ICS department. | | | .625 |
| Extraction Method: Principal Component Analysis. | | | |
| a. 3 components extracted. | | | |

## Awareness of UKZN information systems policies

| KMO and Bartlett's Test | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .698 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 582.229 |
| | df | 6 |
| | Sig. | .000 |

| Component Matrix[a] | |
|---|---|
| | Component |
| | 1 |
| 9.2. I am aware of UKZN policies regarding access to the UKZN network | .914 |
| 9.1. I am aware of UKZN policies regarding physical access to computer rooms/ LAN | .877 |
| 9.3. I am aware of UKZN policies regarding choosing a strong password | .731 |
| 9.4. I do check the ICS website regularly to acquaint myself with new information security alerts | .559 |
| Extracted by Principal Component Analysis | |

## Appendix F – Demographic statistics

### Age

| 1.Age | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Less than 18 | 4 | 1.1 | 1.1 | 1.1 |
| | 18 - 24 | 341 | 90.7 | 90.7 | 91.8 |
| | 25 - 30 | 24 | 6.4 | 6.4 | 98.1 |
| | 31 - Above | 7 | 1.9 | 1.9 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

### Gender

| 2. Gender: | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Female | 169 | 44.9 | 44.9 | 44.9 |
| | Male | 207 | 55.1 | 55.1 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

### Ethnicity

| 3. Ethnicity | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | African | 301 | 80.1 | 80.5 | 80.5 |
| | Indian | 59 | 15.7 | 15.8 | 96.3 |
| | Coloured | 8 | 2.1 | 2.1 | 98.4 |
| | White | 6 | 1.6 | 1.6 | 100.0 |
| | Total | 374 | 99.5 | 100.0 | |
| Missing | 999 | 2 | .5 | | |
| Total | | 376 | 100.0 | | |

### Academic Level

| 4. Academic Level | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | First year | 88 | 23.4 | 23.4 | 23.4 |
| | Second year | 91 | 24.2 | 24.2 | 47.6 |
| | Third year | 136 | 36.2 | 36.2 | 83.8 |
| | Honours | 48 | 12.8 | 12.8 | 96.5 |
| | Masters | 8 | 2.1 | 2.1 | 98.7 |
| | PhD | 5 | 1.3 | 1.3 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

## School

| 5. School | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Management, IT and Governance | 129 | 34.3 | 34.9 | 34.9 |
| | Accounting, Economics and Finance | 121 | 32.2 | 32.7 | 67.6 |
| | Law | 39 | 10.4 | 10.5 | 78.1 |
| | Graduate School of Business and Leadership | 1 | .3 | .3 | 78.4 |
| | Health Science | 20 | 5.3 | 5.4 | 83.8 |
| | College of Agriculture, Engineering and Science | 30 | 8.0 | 8.1 | 91.9 |
| | Life Science | 7 | 1.9 | 1.9 | 93.8 |
| | Math, Stats & CS | 16 | 4.3 | 4.3 | 98.1 |
| | Chemistry & Physics | 3 | .8 | .8 | 98.9 |
| | Humanities | 4 | 1.1 | 1.1 | 100.0 |
| | Total | 370 | 98.4 | 100.0 | |
| Missing | 999 | 6 | 1.6 | | |
| Total | | 376 | 100.0 | | |

## Campus

| 6. Campus | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Pietermaritzburg | 196 | 52.1 | 52.1 | 52.1 |
| | Westville | 180 | 47.9 | 47.9 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

## Appendix G – Descriptive statistics of the constructs

### 7. Physical access to computer rooms

| 7.1. I always use my student card to access computer facilities (LANs) | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 2 | .5 | .5 | .5 |
| | Disagree | 10 | 2.7 | 2.7 | 3.2 |
| | Neither | 12 | 3.2 | 3.2 | 6.4 |
| | Agree | 88 | 23.4 | 23.4 | 29.8 |
| | Strongly Agree | 264 | 70.2 | 70.2 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 7.2. I sometimes ask students to grant me access to computer facilities (LANs) | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 56 | 14.9 | 14.9 | 14.9 |
| | Disagree | 54 | 14.4 | 14.4 | 29.3 |
| | Neither | 71 | 18.9 | 18.9 | 48.3 |
| | Agree | 129 | 34.3 | 34.4 | 82.7 |
| | Strongly Agree | 65 | 17.3 | 17.3 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 7.3. I sometimes let students access the LANs using my student card. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 40 | 10.6 | 10.6 | 10.6 |
| | Disagree | 39 | 10.4 | 10.4 | 21.0 |
| | Neither | 69 | 18.4 | 18.4 | 39.4 |
| | Agree | 152 | 40.4 | 40.4 | 79.8 |
| | Strongly Agree | 76 | 20.2 | 20.2 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

### 8. Access to the University network

| 8.1. I always use my personal login details and password to login into UKZN network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 1 | .3 | .3 | .3 |
| | Disagree | 2 | .5 | .5 | .8 |
| | Neither | 4 | 1.1 | 1.1 | 1.9 |
| | Agree | 39 | 10.4 | 10.4 | 12.2 |
| | Strongly Agree | 330 | 87.8 | 87.8 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 8.2. I sometimes use someone else login details (username and password) to access the university network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 197 | 52.4 | 52.4 | 52.4 |
| | Disagree | 110 | 29.3 | 29.3 | 81.6 |
| | Neither | 20 | 5.3 | 5.3 | 87.0 |
| | Agree | 38 | 10.1 | 10.1 | 97.1 |
| | Strongly Agree | 11 | 2.9 | 2.9 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 8.3. I sometimes allow other people to use my login details (username and password) to access the university network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 168 | 44.7 | 44.7 | 44.7 |
| | Disagree | 117 | 31.1 | 31.1 | 75.8 |
| | Neither | 29 | 7.7 | 7.7 | 83.5 |
| | Agree | 47 | 12.5 | 12.5 | 96.0 |
| | Strongly Agree | 15 | 4.0 | 4.0 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 8.4. I always change my password (to access the University network) at least once in 3 months | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 137 | 36.4 | 36.4 | 36.4 |
| | Disagree | 126 | 33.5 | 33.5 | 69.9 |
| | Neither | 55 | 14.6 | 14.6 | 84.6 |
| | Agree | 45 | 12.0 | 12.0 | 96.5 |
| | Strongly Agree | 13 | 3.5 | 3.5 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 8.5.I always use a password with combination of combination of letters, numbers and symbols (@, #, $, %, etc.) to access the University network as recommended by the UKZN ICS department. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 16 | 4.3 | 4.3 | 4.3 |
| | Disagree | 17 | 4.5 | 4.5 | 8.8 |
| | Neither | 27 | 7.2 | 7.2 | 16.0 |
| | Agree | 115 | 30.6 | 30.6 | 46.5 |
| | Strongly Agree | 201 | 53.5 | 53.5 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 8.6. The password that I use to access the UKZN network is unknown to anyone else. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 24 | 6.4 | 6.4 | 6.4 |
| | Disagree | 32 | 8.5 | 8.5 | 14.9 |
| | Neither | 29 | 7.7 | 7.7 | 22.6 |
| | Agree | 98 | 26.1 | 26.1 | 48.7 |
| | Strongly Agree | 193 | 51.3 | 51.3 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 8.7. I provide my UKZN login details when requested via email | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 133 | 35.4 | 35.4 | 35.4 |
| | Disagree | 53 | 14.1 | 14.1 | 49.5 |
| | Neither | 30 | 8.0 | 8.0 | 57.4 |
| | Agree | 60 | 16.0 | 16.0 | 73.4 |
| | Strongly Agree | 100 | 26.6 | 26.6 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 8.8. I take information security precautionary measures (e.g. frequently changing password, not sharing login details, not click on unknown email links etc.) as advised through the UKZN email alerts. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 29 | 7.7 | 7.7 | 7.7 |
| | Disagree | 36 | 9.6 | 9.6 | 17.3 |
| | Neither | 90 | 23.9 | 24.0 | 41.3 |
| | Agree | 108 | 28.7 | 28.8 | 70.1 |
| | Strongly Agree | 112 | 29.8 | 29.9 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 8.9. I have been a victim of phishing scams (email scams) while using the UKZN network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 160 | 42.6 | 42.9 | 42.9 |
| | Disagree | 107 | 28.5 | 28.7 | 71.6 |
| | Neither | 37 | 9.8 | 9.9 | 81.5 |
| | Agree | 46 | 12.2 | 12.3 | 93.8 |
| | Strongly Agree | 23 | 6.1 | 6.2 | 100.0 |
| | Total | 373 | 99.2 | 100.0 | |
| Missing | 999 | 3 | .8 | | |
| Total | | 376 | 100.0 | | |

## 9. Awareness of UKZN information systems policies

| 9.1. I am aware of UKZN policies regarding physical access to computer rooms/ LAN | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 11 | 2.9 | 2.9 | 2.9 |
| | Disagree | 36 | 9.6 | 9.6 | 12.5 |
| | Neither | 60 | 16.0 | 16.0 | 28.5 |
| | Agree | 164 | 43.6 | 43.6 | 72.1 |
| | Strongly Agree | 105 | 27.9 | 27.9 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 9.2. I am aware of UKZN policies regarding access to the UKZN network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 8 | 2.1 | 2.1 | 2.1 |
| | Disagree | 37 | 9.8 | 9.8 | 12.0 |
| | Neither | 71 | 18.9 | 18.9 | 30.9 |
| | Agree | 166 | 44.1 | 44.1 | 75.0 |
| | Strongly Agree | 94 | 25.0 | 25.0 | 100.0 |

| 9.3. I am aware of UKZN policies regarding choosing a strong password | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 1 | .3 | .3 | .3 |
| | Disagree | 17 | 4.5 | 4.5 | 4.8 |
| | Neither | 44 | 11.7 | 11.7 | 16.5 |
| | Agree | 188 | 50.0 | 50.1 | 66.7 |
| | Strongly Agree | 125 | 33.2 | 33.3 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 9.4. I do check the ICS website regularly to acquaint myself with new information security alerts | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 71 | 18.9 | 18.9 | 18.9 |
| | Disagree | 111 | 29.5 | 29.5 | 48.4 |
| | Neither | 118 | 31.4 | 31.4 | 79.8 |
| | Agree | 48 | 12.8 | 12.8 | 92.6 |
| | Strongly Agree | 28 | 7.4 | 7.4 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

## 10. Perceived Vulnerability

| 10.1 I could be a victim of a serious information security threat | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 31 | 8.2 | 8.3 | 8.3 |
| | Disagree | 60 | 16.0 | 16.0 | 24.3 |
| | Neither | 122 | 32.4 | 32.5 | 56.8 |
| | Agree | 129 | 34.3 | 34.4 | 91.2 |
| | Strongly Agree | 33 | 8.8 | 8.8 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 10.2. UKZN could be subjected to a serious information security threat | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 9 | 2.4 | 2.4 | 2.4 |
| | Disagree | 44 | 11.7 | 11.7 | 14.1 |
| | Neither | 152 | 40.4 | 40.5 | 54.7 |
| | Agree | 132 | 35.1 | 35.2 | 89.9 |
| | Strongly Agree | 38 | 10.1 | 10.1 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 10.3. UKZN faces more and more serious information security threats lately. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 12 | 3.2 | 3.2 | 3.2 |
| | Disagree | 50 | 13.3 | 13.3 | 16.5 |
| | Neither | 189 | 50.3 | 50.4 | 66.9 |
| | Agree | 92 | 24.5 | 24.5 | 91.5 |
| | Strongly Agree | 32 | 8.5 | 8.5 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

## 11. Perceived Severity

| 11.1. An information security breach at UKZN will be a serious problem for me | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 7 | 1.9 | 1.9 | 1.9 |
| | Disagree | 25 | 6.6 | 6.7 | 8.5 |
| | Neither | 79 | 21.0 | 21.1 | 29.6 |
| | Agree | 163 | 43.4 | 43.5 | 73.1 |
| | Strongly Agree | 101 | 26.9 | 26.9 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 11.2. I will lose vital information if my login credential are stolen | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 6 | 1.6 | 1.6 | 1.6 |
| | Disagree | 24 | 6.4 | 6.4 | 8.0 |
| | Neither | 63 | 16.8 | 16.8 | 24.8 |
| | Agree | 164 | 43.6 | 43.7 | 68.5 |
| | Strongly Agree | 118 | 31.4 | 31.5 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 11.3. My privacy will be seriously violated if my login credentials are stolen | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 2 | .5 | .5 | .5 |
| | Disagree | 14 | 3.7 | 3.7 | 4.3 |
| | Neither | 28 | 7.4 | 7.4 | 11.7 |
| | Agree | 162 | 43.1 | 43.1 | 54.8 |
| | Strongly Agree | 170 | 45.2 | 45.2 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 11.4. I will be in serious trouble if someone access the computer rooms using my student card | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 10 | 2.7 | 2.7 | 2.7 |
| | Disagree | 26 | 6.9 | 7.0 | 9.7 |
| | Neither | 97 | 25.8 | 26.0 | 35.7 |
| | Agree | 136 | 36.2 | 36.5 | 72.1 |
| | Strongly Agree | 104 | 27.7 | 27.9 | 100.0 |
| | Total | 373 | 99.2 | 100.0 | |
| Missing | 999 | 3 | .8 | | |
| Total | | 376 | 100.0 | | |

| 11.5. I will be in serious trouble if someone uses my login details to commit cybercrimes using the University network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 3 | .8 | .8 | .8 |
| | Disagree | 7 | 1.9 | 1.9 | 2.7 |
| | Neither | 25 | 6.6 | 6.7 | 9.4 |
| | Agree | 107 | 28.5 | 28.6 | 38.0 |
| | Strongly Agree | 232 | 61.7 | 62.0 | 100.0 |
| | Total | 374 | 99.5 | 100.0 | |
| Missing | 999 | 2 | .5 | | |
| Total | | 376 | 100.0 | | |

## 12. Perceived rewards

| 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 91 | 24.2 | 24.3 | 24.3 |
| | Disagree | 163 | 43.4 | 43.5 | 67.7 |
| | Neither | 96 | 25.5 | 25.6 | 93.3 |
| | Agree | 22 | 5.9 | 5.9 | 99.2 |
| | Strongly Agree | 3 | .8 | .8 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |


| 12.2. I would feel rewarded if a friend uses my LAN credentials to access the university network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 91 | 24.2 | 24.3 | 24.3 |
| | Disagree | 163 | 43.4 | 43.5 | 67.7 |
| | Neither | 96 | 25.5 | 25.6 | 93.3 |
| | Agree | 22 | 5.9 | 5.9 | 99.2 |
| | Strongly Agree | 3 | .8 | .8 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |


| 12.3. I benefit from NOT complying (e.g. watching movies online, sharing login details etc.) with the university security measures than by complying with them. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 60 | 16.0 | 16.0 | 16.0 |
| | Disagree | 108 | 28.7 | 28.8 | 44.8 |
| | Neither | 116 | 30.9 | 30.9 | 75.7 |
| | Agree | 60 | 16.0 | 16.0 | 91.7 |
| | Strongly Agree | 31 | 8.2 | 8.3 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

## 13. Response Efficacy

| 13.1. I believe that NOT sharing my LAN login details prevents or reduces chances of identity theft. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 2 | .5 | .5 | .5 |
| | Disagree | 9 | 2.4 | 2.4 | 2.9 |
| | Neither | 23 | 6.1 | 6.1 | 9.0 |
| | Agree | 145 | 38.6 | 38.6 | 47.6 |
| | Strongly Agree | 197 | 52.4 | 52.4 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 13.2. I believe that NOT sharing my student card helps to reduce security breaches. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 2 | .5 | .5 | .5 |
| | Disagree | 13 | 3.5 | 3.5 | 4.0 |
| | Neither | 34 | 9.0 | 9.0 | 13.0 |
| | Agree | 157 | 41.8 | 41.8 | 54.8 |
| | Strongly Agree | 170 | 45.2 | 45.2 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 13.3. If I comply with information security policies, Information Systems security breaches will be scarce. | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 1 | .3 | .3 | .3 |
| | Disagree | 12 | 3.2 | 3.2 | 3.5 |
| | Neither | 62 | 16.5 | 16.5 | 19.9 |
| | Agree | 149 | 39.6 | 39.6 | 59.6 |
| | Strongly Agree | 152 | 40.4 | 40.4 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

## 14. Self-efficacy

| 14.1. I can comply with UKZN information security measures by myself | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 2 | .5 | .5 | .5 |
| | Disagree | 15 | 4.0 | 4.0 | 4.5 |
| | Neither | 56 | 14.9 | 14.9 | 19.4 |
| | Agree | 199 | 52.9 | 52.9 | 72.3 |
| | Strongly Agree | 104 | 27.7 | 27.7 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 14.2. I need assistance to comply with UKZN information security measures | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 31 | 8.2 | 8.2 | 8.2 |
| | Disagree | 130 | 34.6 | 34.6 | 42.8 |
| | Neither | 106 | 28.2 | 28.2 | 71.0 |
| | Agree | 94 | 25.0 | 25.0 | 96.0 |
| | Strongly Agree | 15 | 4.0 | 4.0 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 14.3. I am not confident enough to comply with UKZN information security measures | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 45 | 12.0 | 12.0 | 12.0 |
| | Disagree | 151 | 40.2 | 40.3 | 52.3 |
| | Neither | 110 | 29.3 | 29.3 | 81.6 |
| | Agree | 49 | 13.0 | 13.1 | 94.7 |
| | Strongly Agree | 20 | 5.3 | 5.3 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

## 15. Response Cost

| 15.1. Complying with information security measures is an inconvenience to me | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 50 | 13.3 | 13.3 | 13.3 |
| | Disagree | 182 | 48.4 | 48.4 | 61.7 |
| | Neither | 95 | 25.3 | 25.3 | 87.0 |
| | Agree | 38 | 10.1 | 10.1 | 97.1 |
| | Strongly Agree | 11 | 2.9 | 2.9 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 15.2. Complying with information security measures is time consuming | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 50 | 13.3 | 13.3 | 13.3 |
| | Disagree | 165 | 43.9 | 43.9 | 57.2 |
| | Neither | 93 | 24.7 | 24.7 | 81.9 |
| | Agree | 47 | 12.5 | 12.5 | 94.4 |
| | Strongly Agree | 21 | 5.6 | 5.6 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 15.3. Complying with information security measures requires a lot of effort other than time | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 58 | 15.4 | 15.4 | 15.4 |
| | Disagree | 143 | 38.0 | 38.0 | 53.5 |
| | Neither | 100 | 26.6 | 26.6 | 80.1 |
| | Agree | 56 | 14.9 | 14.9 | 94.9 |
| | Strongly Agree | 19 | 5.1 | 5.1 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

## 16. Challenges to information security compliance

| 16.1. I do not have the required IT skills to comply with UKZN information security measures | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 69 | 18.4 | 18.4 | 18.4 |
| | Disagree | 162 | 43.1 | 43.2 | 61.6 |
| | Neither | 75 | 19.9 | 20.0 | 81.6 |
| | Agree | 54 | 14.4 | 14.4 | 96.0 |
| | Strongly Agree | 15 | 4.0 | 4.0 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 62 | 16.5 | 16.5 | 16.5 |
| | Disagree | 108 | 28.7 | 28.7 | 45.2 |
| | Neither | 98 | 26.1 | 26.1 | 71.3 |
| | Agree | 88 | 23.4 | 23.4 | 94.7 |
| | Strongly Agree | 20 | 5.3 | 5.3 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 16.3. I do not know how to change the password that I use to access the UKZN network | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 114 | 30.3 | 30.4 | 30.4 |
| | Disagree | 181 | 48.1 | 48.3 | 78.7 |
| | Neither | 36 | 9.6 | 9.6 | 88.3 |
| | Agree | 32 | 8.5 | 8.5 | 96.8 |
| | Strongly Agree | 12 | 3.2 | 3.2 | 100.0 |
| | Total | 375 | 99.7 | 100.0 | |
| Missing | 999 | 1 | .3 | | |
| Total | | 376 | 100.0 | | |

| 16.4. I am not aware of ICS policy with regard to the use of password | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 53 | 14.1 | 14.1 | 14.1 |
| | Disagree | 147 | 39.1 | 39.1 | 53.2 |
| | Neither | 80 | 21.3 | 21.3 | 74.5 |
| | Agree | 72 | 19.1 | 19.1 | 93.6 |
| | Strongly Agree | 24 | 6.4 | 6.4 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 65 | 17.3 | 17.3 | 17.3 |
| | Disagree | 152 | 40.4 | 40.4 | 57.7 |
| | Neither | 83 | 22.1 | 22.1 | 79.8 |
| | Agree | 58 | 15.4 | 15.4 | 95.2 |
| | Strongly Agree | 18 | 4.8 | 4.8 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 16.6. I am not informed about the latest phishing scams (email scams) | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 74 | 19.7 | 19.7 | 19.7 |
| | Disagree | 123 | 32.7 | 32.7 | 52.4 |
| | Neither | 71 | 18.9 | 18.9 | 71.3 |
| | Agree | 77 | 20.5 | 20.5 | 91.8 |
| | Strongly Agree | 31 | 8.2 | 8.2 | 100.0 |
| | Total | 376 | 100.0 | 100.0 | |

| 16.7. I am not informed about the latest cybersecurity crimes | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Strongly Disagree | 63 | 16.8 | 16.8 | 16.8 |
| | Disagree | 113 | 30.1 | 30.2 | 47.1 |
| | Neither | 77 | 20.5 | 20.6 | 67.6 |
| | Agree | 81 | 21.5 | 21.7 | 89.3 |
| | Strongly Agree | 40 | 10.6 | 10.7 | 100.0 |
| | Total | 374 | 99.5 | 100.0 | |
| Missing | 999 | 2 | .5 | | |
| Total | | 376 | 100.0 | | |

## Appendix H – Correlation and Regression Tests

### Research Question 3

Correlation: Self-efficacy physical access factor 1

| | | Q7 Physical access to computer rooms |
|---|---|---|
| Q7 Physical access to computer rooms | Pearson Correlation | 1 |
| | Sig. (2-tailed) | |
| | N | 375 |
| 14.1. I can comply with UKZN information security measures by myself | Pearson Correlation | -.039 |
| | Sig. (2-tailed) | .455 |
| | N | 375 |
| 14.2. I need assistance to comply with UKZN information security measures | Pearson Correlation | .050 |
| | Sig. (2-tailed) | .336 |
| | N | 375 |
| 14.3. I am not confident enough to comply with UKZN information security measures | Pearson Correlation | .056 |
| | Sig. (2-tailed) | .278 |
| | N | 374 |

Regression: Self-efficacy network access factor 2

Coefficients[a]

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | -.899 | .361 | | -2.489 | .013 |
| | 14.1. I can comply with UKZN information security measures by myself | .108 | .068 | .086 | 1.599 | .111 |
| | 14.2. I need assistance to comply with UKZN information security measures | .145 | .060 | .149 | 2.432 | .015 |
| | 14.3. I am not confident enough to comply with UKZN information security measures | .021 | .059 | .021 | .355 | .722 |

a. Dependent Variable: Q8 Access to the University network f2

Correlation: response-cost physical access factor 1

| | | | Q7 Physical access to computer rooms |
|---|---|---|---|
| Spearman's rho | Q7 Physical access to computer rooms | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 375 |
| | 14.1. I can comply with UKZN information security measures by myself | Correlation Coefficient | -.038 |
| | | Sig. (2-tailed) | .463 |
| | | N | 375 |
| | 14.2. I need assistance to comply with UKZN information security measures | Correlation Coefficient | .030 |
| | | Sig. (2-tailed) | .561 |
| | | N | 375 |
| | 14.3. I am not confident enough to comply with UKZN information security measures | Correlation Coefficient | .043 |
| | | Sig. (2-tailed) | .409 |
| | | N | 374 |

Regression: Response Cost network access factor 2

| Coefficients | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardised Coefficient | | Standardized Coefficient | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constants) | -.187 | .155 | | -1.200 | .231 |
| | 15.1. Complying with information security measures is an inconvenience to me | -.062 | .072 | -.059 | -.857 | .392 |
| | 15.2. Complying with information security measures is time consuming | -.001 | .077 | -.002 | -.019 | .985 |
| | 15.3. Complying with information security measures requires a lot of effort other than time | .133 | .069 | .144 | 1.926 | .055 |
| a. Dependent Variable: Q8 Access to the University network f2 | | | | | | |

Regression: Response Cost network access factor 3

| Coefficient | | | | | | |
|---|---|---|---|---|---|---|
| Models | | Unstandardised Coefficients | | Standardised Coefficient | t | Sig. |
| | | B | Std. Error | Beta | | |
| 1 | (Constants) | .364 | .155 | | 2.345 | .020 |
| | 15.1. Complying with information security measures is an inconvenience to me | -.098 | .072 | -.093 | -1.363 | .174 |
| | 15.2. Complying with information security measures is time consuming | .035 | .077 | .037 | .455 | .649 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 15.3. Complying with information security measures requires a lot of effort other than time | -.084 | .069 | -.091 | -1.222 | .223 |
| a. Dependent Variable: Q8 Access to the University network f3 | | | | | | |

## Research Question 4

Correlation: physical access factor 1

| Correlation | | | Q7 Physical access to computer rooms |
|---|---|---|---|
| Spearman's rho | Q7 Physical access to computer rooms | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 375 |
| | 16.1. I do not have the required IT skills to comply with UKZN information security measures | Correlation Coefficient | .095 |
| | | Sig. (2-tailed) | .067 |
| | | N | 374 |
| | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | Correlation Coefficient | .186** |
| | | Sig. (2-tailed) | .000 |
| | | N | 375 |
| | 16.3. I do not know how to change the password that I use to access the UKZN network | Correlation Coefficient | .131* |
| | | Sig. (2-tailed) | .011 |
| | | N | 374 |
| | 16.4. I am not aware of ICS policy with regard to the use of password | Correlation Coefficient | .169** |
| | | Sig. (2-tailed) | .001 |
| | | N | 375 |
| | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | Correlation Coefficient | .225** |
| | | Sig. (2-tailed) | .000 |
| | | N | 375 |
| | 16.6. I am not informed about the latest phishing scams (email scams) | Correlation Coefficient | .091 |
| | | Sig. (2-tailed) | .080 |
| | | N | 375 |
| | 16.7. I am not informed about the latest cybersecurity crimes | Correlation Coefficient | .041 |
| | | Sig. (2-tailed) | .434 |
| | | N | 373 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

Regression: physical access factor 1

| Coefficients[a] | | | | | |
|---|---|---|---|---|---|
| Model | Unstandardised Coefficient | | Standardised Coefficient | t | Sig. |
| | B | Std. Error | Beta | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | (Constant) | -.601 | .174 | | -3.449 | .001 |
| | 16.1. I do not have the required IT skills to comply with UKZN information security measures | -.111 | .068 | -.118 | -1.633 | .103 |
| | 16.2. I do not have enough cybersecurity knowledge to comply with UKZN information security measures in place | .172 | .062 | .199 | 2.763 | .006 |
| | 16.3. I do not know how to change the password that I use to access the UKZN network | .045 | .056 | .046 | .809 | .419 |
| | 16.4. I am not aware of ICS policy with regard to the use of password | .052 | .059 | .058 | .874 | .383 |
| | 16.5. I am not aware of ICS/UKZN policy with regard to accessing computer rooms (LANs) | .150 | .062 | .165 | 2.408 | .017 |
| | 16.6. I am not informed about the latest phishing scams (email scams) | .061 | .073 | .076 | .837 | .403 |
| | 16.7. I am not informed about the latest cybersecurity crimes | -.133 | .070 | -.168 | -1.896 | .059 |
| a. Dependent Variable: Q7 Physical access to computer rooms | | | | | | |

# REFERENCES


Abulela, M. A., & Harwell, M. (2020). Data analysis: Strengthening inferences in quantitative education studies conducted by novice researchers. *Educational Sciences: Theory & Practice*, *20*(1), 59-78.

Ahmed, M., Sharif, L., Kabir, M., & Al-Maimani, M. (2012). Human errors in information security. *International Journal*, *1*(3), 82-87.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Al-Haijaa, Q. A., & Ishtaiwia, A. (2021). Machine learning based model to identify firewall decisions to improve cyber-defense. *International Journal on Advanced Science, Engineering and Information Technology*, *11*(4), 1688-1695.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73.

Algarni, A., Ahmad, M., Attaallah, A., Agrawal, A., Kumar, R., & Khan, R. A. (2020). A hybrid fuzzy rule-based multi-criteria framework for security assessment of medical device software. *International Journal of Intelligent Engineering and Systems*, *13*(5), 51-62.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23.

Ali, R. F., Dominic, P., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, *11*(8), 3383.

Alnatheer, M. A. (2015, 13-15 April 2015). Information Security Culture Critical Success Factors. 2015 12th International Conference on Information Technology - New Generations,

Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *Ieee Access*, *8*, 165130-165150.

Anderson, R., & Barton, C. (2012). B¨ohme R., Clayton R., van Eeten M., Levi M., Moore T., Savage S.: Measuring the Cost of Cybercrime.

Apuke, O. D. (2017). Quantitative research methods: A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, *33*(5471), 1-8.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bakar, R. A., Rahmatullah, B., Munastiwi, E., & Dheyab, O. (2021). A confirmatory analysis of the prevention insider threat in organization information system. *Journal of Technology and Humanities*, *2*(1), 20-30.

Barbera, J., Naibert, N., Komperda, R., & Pentecost, T. C. (2020). Clarity on Cronbach's Alpha Use. *Journal of Chemical Education*, *98*(2), 257-258.

Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *48*(3), 44-68.

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

Bhardwaj, P. (2019). Types of sampling in research. *Journal of the Practice of Cardiovascular Sciences*, *5*(3), 157.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices.
Bloomfield, J., & Fisher, M. J. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses Association*, *22*(2), 27-30.
Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors.
Bulbulia, & Maharaj. (2013). ii

Factors that influence young adults‟ online security awareness.
Burns, A., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209.
Cancino-Montecinos, S., Björklund, F., & Lindholm, T. (2020). A general model of dissonance reduction: unifying past accounts via an emotion regulation perspective. *Frontiers in psychology*, *11*, 540081.
Casula, M., Rangarajan, N., & Shields, P. (2021). The potential of working hypotheses for deductive exploratory research. *Quality & Quantity*, *55*(5), 1703-1725.
Chan, H., & Mubarak, S. (2012). Significance of information security awareness in the higher education sector. *International Journal of Computer Applications*, *60*(10).
Chandra, N. A., Ramli, K., Ratna, A. A. P., & Gunawan, T. S. (2022). Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. *Risks*, *10*(8), 165. https://www.mdpi.com/2227-9091/10/8/165
Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *computers & security*, *39*, 447-459.
Chenoweth, Minch, & Gattiker. (2009). Application of Protection Motivation Theory

to Adoption of Protective Technologies. *Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009*.
Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31.
Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *psychometrika*, *16*(3), 297-334.
D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*.
da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162-176. https://doi.org/https://doi.org/10.1016/j.cose.2014.12.006
Daneshmandnia, A. (2019). The influence of organizational culture on information governance effectiveness. *Records Management Journal*.
Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.
Dheri, G., Pal, S., Singh, V., Marwaha, S., & Choudhary, O. (2019). Hands-on Training on "Statistical Tools and Database Management In Agriculture" [ Compendium]. 106 - 110. (ICAR NAHEP-CAAST-SNRM DEPARTMENT OF SOIL SCIENCE)
Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *information security technical report*, *14*(4), 223-229.
Empey, C., & Latto, N. (2022, 22 July 2022). *What Is a VPN & How Does It Work?* https://www.avast.com/c-what-is-a-vpn
Explorable. (2016). *Research Population*. https://explorable.com/research-population

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond. *Journal of the Association for Information Systems*, *20*(11), 2.

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

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), 407-429.

Foltz, B., & Hauser, R. (2005). Faculty awareness of university computer usage regulations.

Frey, L., Botan, C. H., & Kreps, G. (2000). Investigating communication. *NY: Allyn & Bacon*.

Ghazvini, & Shukur. (2017). Review of information security guidelines for awareness training program in healthcare industry. *6th International Conference on Electrical Engineering and Informatics (ICEEI)*.

Guillot, A., & Kennedy, S. (2007). Information Security Surveys: A Review of the Methodologies, the Critics and a. Australian Information Security Management Conference,

Gümüşbaş, D., Yıldırım, T., Genovese, A., & Scotti, F. (2020). A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. *IEEE Systems Journal*, *15*(2), 1717-1731.

Gundu, T., & Flowerday, S. V. (2013). IGNORANCE TO AWARENESS: TOWARDS AN INFORMATION SECURITY AWARENESS PROCESS *Vol.104(2)*.

Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *52*(2), 25-67.

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior.

Hale, J., & Brusil, P. (2007). Secur (e/ity) management: A continuing uphill climb. *Journal of Network and Systems Management*, *15*(4), 525-553.

Hamid, H., & Zeki, A. M. (2014). Users' Awareness of and Perception on Information Security Issues: A Case Study of Kulliyyah of ICT Postgraduate Students. Advanced Computer Science Applications and Technologies (ACSAT), 2014 3rd International Conference on,

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

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

Hina, S., & Dominic, D. D. (2016). Information security policies: Investigation of compliance in universities. 2016 3rd International Conference on Computer and Information Sciences (ICCOINS),

Hina, S., & Dominic, D. D. (2017, 16-17 July 2017). Need for information security policies compliance: A perspective in Higher Education Institutions. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS),

Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*, *60*(3), 201-211.

Hina, S., Selvam, D. D. D. P., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, 101594.

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

Igbaria, M., & Iivari, J. (1995). The effects of self-efficacy on computer usage. *Omega*, *23*(6), 587-605.

Information & Communication Services. (2022). *University of KwaZulu-Natal Information & Communication Services*. https://ics.ukzn.ac.za/

Information & Communication Services, U. o. K.-N. (2018). Retrieved 2018 from https://www.ics.ukzn.ac.za

Jayanti, R. K., & Burns, A. C. (1998). The antecedents of preventive health care behavior: An empirical study. *Journal of the academy of marketing science*, *26*(1), 6-15.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, 549-566.

Joshi, P. (2019). Research design. In *Research Methodology* (pp. 69-98). Chapman and Hall/CRC.

Karjalainen, M. (2011). Improving employees' information systems (IS) security behaviour: toward a meta-theory of is security training and a new framework for understanding employees' is security behaviour. *PhD. Oulu: The University of Oulu*.

Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. *IEEE Access*, *8*, 52018-52027.

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal: A Global Perspective*, *22*(4), 171-179. https://doi.org/10.1080/19393555.2013.828803

Knekta, E., Runyon, C., & Eddy, S. (2019). One size doesn't fit all: Using factor analysis to gather validity evidence when using surveys in your research. *CBE—Life Sciences Education*, *18*(1), rm1.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and psychological measurement*, *30*(3), 607-610.

Kyobe, M. (2010). Towards a framework to guide compliance with IS Security policies and Regulations in a university. 2010 Information Security for South Africa,

Labaree, R. V. (2009). Research Guides: Organizing Your Social Sciences Research Paper: Qualitative Methods.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4-13.

Laerd, S. (2013). Pearson product-moment correlation. *Retrieved from*.

Laerd, S. (2022). *Principal Components Analysis (PCA) using SPSS Statistics*. Laerd statistics. https://statistics.laerd.com/spss-tutorials/principal-components-analysis-pca-using-spss-statistics.php

Lane, T. (2007). *Information security management in Australian universities : an exploratory analysis*

Queensland University of Technology]. https://eprints.qut.edu.au/16486/

LaRose, R., Rifon, N. J., & Wirth, C. (2007). Online safety begins with you and me: getting Internet users to protect themselves. Annual conference of the International Communication Association (ICA 2007),

Latham, B. (2007). Sampling: What is it? Quantitative research methods. *International Journal of Technology Enhancements and Emerging Enginerring Research*, *3*(5), 44-55.

Leech, N. L., Barrett, K. C., & George, A. (2005). Morgan (2005). *SPSS for intermediate statistics: Use and interpretation*.

Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using Leximancer for qualitative data analysis triangulation. *The Qualitative Report*, *25*(3), 604-614.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

Masrek, M. N. (2017, 18-19 Oct. 2017). Assessing information security culture: The case of Malaysia public organization. 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE),

Matveev, A. V. (2002). The advantages of employing quantitative and qualitative methods in intercultural research: Practical implications from the study of the perceptions of intercultural communication competence by American and Russian managers. *Theory of communication and applied communication*, *1*(6), 59-67.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce*, *9*(1), 23-41. https://doi.org/10.1080/15332861.2010.487415

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, *30*(7), 537-542.

McIlwraith, A. (2006). Information Security and Employee Behaviour. (Aldershot, Hampshire, UK)

Mendonça, R. V., Teodoro, A. A., Rosa, R. L., Saadi, M., Melgarejo, D. C., Nardelli, P. H., & Rodríguez, D. Z. (2021). Intrusion detection system based on fast hierarchical deep convolutional neural network. *IEEE Access*, *9*, 61024-61034.

Mohammed, A. (2015). Information security culture critical success factors. 2015 12th International Conference on Information Technology-New Generations,

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. *Journal of the Association for Information Systems*, *23*(1), 196-236.

Muijs, D. (2010). *Doing quantitative research in education with SPSS*. Sage.

Murphy, K., Tyler, T., & Curtis, A. (2009). Nurturing Regulatory Compliance: Is Procedural Justice Effective When People Question the Legitimacy of the Law? *Regulation & Governance*, *3*, 1-26. https://doi.org/10.1111/j.1748-5991.2009.01043.x

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

Ngo, L., Zhou, W., Chonka, A., & Singh, J. (2009, 3-5 Nov. 2009). Assessing the level of I.T. security culture improvement: Results from three Australian SMEs. 2009 35th Annual Conference of IEEE Industrial Electronics,

Nickolas, S. (2021). *What Do Correlation Coefficients Positive, Negative, and Zero Mean?* https://www.investopedia.com/ask/answers/032515/what-does-it-mean-if-correlation-coefficient-positive-negative-or-zero.asp

Ormond, D., Warkentin, M., & Crossler, R. E. (2019). Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems*, *20*(12), 4.

Osbaldeston, A. (2021). *5 Reasons To Combine Qualitative And Quantitative Research*. questback. https://www.questback.com/blog/5-reasons-to-combine-qualitative-and-quantitative-research/

Pahnila, S., Siponen, M., & Mahmood, A. (2007, 3-6 Jan. 2007). Employees' Behavior towards IS Security Policy Compliance. 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07),

Pallant, J. (2013). *SPSS survival manual*. McGraw-Hill Education (UK).

Pandey, P., & Pandey, M. M. (2021). *Research methodology tools and techniques*. Bridge Center.

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

Prajapati, P., & Shah, P. (2022). A review on secure data deduplication: Cloud storage security issue. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 3996-4007.

Prasetyo, Y. T., Castillo, A. M., Salonga, L. J., Sia, J. A., & Seneta, J. A. (2020). Factors affecting perceived effectiveness of COVID-19 prevention measures among Filipinos during enhanced community quarantine in Luzon, Philippines: Integrating Protection Motivation Theory and extended Theory of Planned Behavior. *International journal of infectious diseases*, *99*, 312-323.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Puniya, M., & Singh, R. Correlation and Regression Analysis.

Rengganis, A., & Katmini, K. (2021). Application of Theory of Planned Behavior on the Implementation of the Emo Demo Creation of Healthy PMT with Full Nutrition in Posyandu Gedang–Gedang Village Batuputih Sumenep. *Journal for Quality in Public Health*, *5*(1), 19-26.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Schafer, J. L., & Olsen, M. K. (1998). Multiple imputation for multivariate missing-data problems: A data analyst's perspective. *Multivariate behavioral research*, *33*(4), 545-571.

Schein, E. H. (2009). *The corporate culture survival guide* (Vol. 158). John Wiley & Sons.

Schrepp, M. (2020). On the Usage of Cronbach's Alpha to Measure Reliability of UX Scales. *Journal of Usability Studies*, *15*(4).

Shahri, A. B., Ismail, Z., & Rahim, N. (2012). Security effectiveness in health information system: through improving the human factors by education and training. *Australian Journal of Basic and Applied Sciences*, *6*(12), 226-233.

Shambabi, P. T., Musarurwa, S., & Shava, F. B. (2021). Assessing Organisational Information Security Culture Among Workforce in Universities: A Case of Namibia. 2021 IST-Africa Conference (IST-Africa),

Sharma, D., Wason, V., & Johri, P. (2021, 4-5 March 2021). Optimized Classification of Firewall Log Data using Heterogeneous Ensemble Techniques. 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE),

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100. https://doi.org/https://doi.org/10.1016/j.compedu.2008.06.011

Shields, P. M., & Rangarajan, N. (2013). *A playbook for research methods: Integrating conceptual frameworks and project management*. New Forums Press.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2).

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *Int. J. Inf. Secur. Priv.*, *9*, 26-46.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *computers & security*, *24*(2), 124-133.

Steinbart, P. J., Keith, M. J., & Babb, J. (2016). Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Information Systems Research*, *27*(2), 219-239.

Sun, Y. (2016, 15-17 April 2016). The Study on Network Information Security. 2016 International Conference on Network and Information Systems for Computers (ICNISC),

Sürücü, L., & Maslakçi, A. (2020). Validity and reliability in quantitative research. *Business & Management Studies: An International Journal*, *8*(3), 2694-2726.

Tanni, T. I., Taharat, T., Parvez, M. S., Rumee, S. T. A., & Zaber, M. I. (2022). Is My Password Strong Enough?: A Study on User Perception in The Developing World. *EAI Endorsed Transactions on Creative Technologies*, *9*(30), e3-e3.

Thomas, J., & Galligher, G. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science*, *11*(1).

Tianxiao, L., Qiang, F., Shuqin, X., & Fanxiang, M. (2009, 14-16 Aug. 2009). Application of Principal Component Analysis in Evaluating Influence Factors of Evaporation in Northern Cold Area. 2009 Fifth International Conference on Natural Computation,

Tribbensee, N. (2003). Liability for negligent security: Implications for policy and practice. *EDUCAUSE REVIEW*, *38*, 48-58.

Trochim, W. (2006). *Sampling*. http://www.socialresearchmethods.net/kb/sampling.php

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. https://doi.org/https://doi.org/10.1016/j.cose.2016.02.009

Tu, Z., & Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management : A Literature Review Completed Research Paper.

UKZN Institutional Intelligence Report. (2022). *University of KwaZulu-Natal Institutional Intelligence Report*. https://ii.ukzn.ac.za/

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

Vestad, A. (2022). Personality Traits and Security Motivation. In (Vol. 299). https://doi.org/10.3233/SHTI220980

Waly, N., Tassabehji, R., & Kamala, M. (2012, 25-27 June 2012). Improving Organisational Information Security Management: The Impact of Training and Awareness. 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems,

Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016),

Wen, C., Li, X., Zanotti, T., Puglisi, F. M., Shi, Y., Saiz, F., Antidormi, A., Roche, S., Zheng, W., & Liang, X. (2021). Advanced Data Encryption using 2D Materials. *Advanced Materials*, *33*(27), 2100185.

Wheelus, C., & Zhu, X. (2020). IoT network security: threats, risks, and a data-driven defense framework. *IoT*, *1*(2), 259-285.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816.

Wu, Y., Stanton, B. F., Li, X., Galbraith, J., & Cole, M. L. (2005). Protection motivation theory and adolescent drug trafficking: relationship between health motivation and longitudinal risk involvement. *Journal of pediatric psychology 30 2*, 127-137 .

Yildirim, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741-759.

Zimba, A., Wang, Z., & Simukonda, L. (2018). Towards data resilience: The analytical case of crypto ransomware data recovery techniques. *International Journal of Information Technology & Computer Science*, *10*(1), 40-51.