EPiC Series in Education Science

Volume 5, 2023, Pages 1–16

Proceedings of NEMISA Digital Skills Conference 2023: Scaling Data Skills For Multidisciplinary Impact

Factors Affecting how University Students Comply with Cybersecurity Measures: A Case of South Africa

Papama Mtambeka[1], Chimwemwe Queen Mtegha[1], Wallace Chigona[1] and Teofelus Tonateni Tuyeni[1]

[1]University of Cape Town, Rondebosch, Cape Town, South Africa

mtmpap001@myuct.ac.za, mtgchi003@myuct.ac.za, wallace.chigona@uct.ac.za, tynteo002@myuct.ac.za

Abstract

Universities across the globe are experiencing a surge of cyberattacks due to the increased usage of information communication technologies (ICTs). To counteract cyberattacks, universities have implemented cybersecurity measures to ensure that students and the universities' critical infrastructures are protected. Unfortunately, universities in developing countries continue to face increased cyberattacks despite implementing cybersecurity measures. This study explores the factors that affect students' compliance with universities' cybersecurity measures.

The study used a case of the University of Cape Town in South Africa, adopting qualitative research and an interpretive paradigm. We used a deductive approach to theory using Protection Motivation Theory (PMT) as the lens for inquiry. The sample for the study consisted of 40 participants, of which 35 were students and five were staff members of the University. The sample of the study was selected by convenience. We collected empirical data from the participants using semi-structured interviews. The data was then analysed using thematic analysis on NVivo software. The study found that students' compliance with cybersecurity measures is affected by their perceptions of the seriousness of the threats, the likelihood of the threats happening, their ability to protect themselves against threat, their belief in the effectiveness of the recommended solutions against cyber threats, and the costs associated with compliance to cybersecurity measures. When students perceive the risk as not severe enough to worry about, they do not find it necessary to comply with the University's cybersecurity measures. Similarly, when the students deem that the recommended compliance actions will not be practical or affordable, they do not adhere to the university cybersecurity measures.

Keywords: Protection Motivation Theory, University, Students, Cybersecurity Measures, Compliance

1 Introduction

With the rapid development and adoption of new technologies come new avenues for criminals to direct their cyberattacks as the number of potential victims increases (Gwebu et al., 2020). Cyberattack is defined as targeted attacks on computer systems with the aim of compromising the confidentiality, integrity and availability of data (Bendovschi, 2015). Therefore, organisations must implement and comply with cybersecurity measures to prevent cyberattacks (Khader et al., 2021). Cybersecurity is the protection of digital information assets from any attacks that may arise through internet usage (Von Solms & Von Solms, 2018). Universities are one of the main targets of cybersecurity threat, due to the substantial amounts of information they hold (Taha & Dahabiyeh, 2021). Research shows that between 2005 to 2021, higher education institutions experienced 1850 data breaches worldwide (Lukehart, 2022). In addition, universities use cyberspace platforms, such as student portals, and communication platforms, such as Microsoft teams, to manage various activities, such as admissions, examinations, administration, finances, and records, to facilitate the educational process (Li et al., 2019).

Despite the apparent advantages of automated processes that cyberspaces offer universities, they also pose cybersecurity threats and challenges to operations and information (Li et al., 2019). The increase in the recurrence of cyberattacks on universities' ICT infrastructures has led to the loss of sensitive information, finances, as well as social and intellectual property (Alharbi & Tassaddiq, 2021). The risk has increased in universities, especially in developing countries, for instance, South Africa, as the management of cyberspaces and resources is poor (Kabanda et al., 2018). In addition, South Africa has the third-highest cybercrimes in the world (Hubbard, 2019).

Despite being aware of the cybersecurity risk, some students do not comply with the universities' cybersecurity measures, such as policies on anti-virus, information and security passwords, internet and email use. These risks can be detrimental to a universities' information systems (Moallem, 2019). Given the rise in cyberattacks and the vulnerability of universities to cyberattacks, there is a need for research investigating the compliance behaviour of students with cybersecurity measures, as they are one of the primary users of university information systems. Unfortunately, there is still a dearth of studies on cybersecurity compliance in developing countries. Therefore, there is a need for more research on how students comply with cybersecurity. With this background, the study aims to answer the following question:

What factors affect students' compliance with Universities' cybersecurity measures?

We used the case of the University of Cape Town (UCT) to respond to the research question. We selected the University out of convenience. A deductive approach to theory was employed using protection motivation theory (PMT). We collected data through semi-structured interviews with students and staff from the department responsible for maintaining the ICT infrastructure of the University.

The study extends available knowledge in this regard, as literature is scarce on those factors that affect students' cybersecurity compliance. Further to this, the findings from the study will inform decision and policymakers in universities on how to implement cybersecurity measures to ensure compliance with the minimal cybersecurity measures.

2 Literature Review

2.1 Cybersecurity

Cybersecurity has risen in significance in recent years due to the increased reliance on and adoption of information communication technologies (ICTs) (Alharbi & Tassaddiq, 2021). Cybersecurity threats are ubiquitous and may affect all organisations across industries, which may be costly (Al Moshaigeh et al., 2019). It is estimated that cybercrime will cost the global economy USD10.5 trillion from 2025 onward (Sausalito, 2020). The main reason for the worldwide trend of cybersecurity challenges is that most users do not follow their organisation's cybersecurity measures (Jeyaraj & Zadeh, 2020). Even though executive awareness of cybersecurity is expanding, most organisations remain inactive, whereas they would be more successful in dealing with cyberthreats if they were proactive. Personalising the risks for users would be beneficial, so that they know their susceptibility and the consequences of their non-compliance (Ergen et al., 2021).

While cybersecurity challenges are not new, the Covid-19 pandemic has significantly exacerbated these threats (Traxler et al., 2020). Covid-19 has shown a surge in cybercrime due to increased dependency on cyberspace, caused by the move towards virtual learning and working across the world (Traxler et al., 2020). In addition, the outbreak of the Covid-19 pandemic saw the emergence of more than 4,000 malicious websites within the first month of the pandemic in 2020, which is in correlation with the move towards virtual work that can be observed as people practised social distancing (Morgan, 2020).

2.2 Cybersecurity Challenges in Africa

Africa has one of the fastest internet penetration rates worldwide. This has resulted in an increasing trend of cyberattacks (Eboibi, 2020). Africa is perceived as the hub for cybercrime and cybercriminals due to the poor response to curb cybersecurity issues (Kabanda et al., 2018; Kshetri, 2019). The high rate of cybercrime on the continent has lowered Africa's GDP by more than 10%, costing the continent US$ 4.12 billion (Interpol, 2021). Online scams are the continent's most common and pressing cyber threats (Interpol, 2021). This entails the theft of personal information and banking information, which a threat actor subsequently uses to buy goods or services, siphon funds, or sell on the open market (Interpol, 2021).

Despite these developments, there is little research on cybersecurity issues in African countries (Kabanda et al., 2018). Along with these challenges, the continent faces a severe cybersecurity workforce shortage due to economic and institutional barriers (Kshetri, 2019). However, African countries have implemented cybercrime legal frameworks and policies in order to mitigate this issue, despite their obstacles, but have failed to enforce those policies (Eboibi, 2020).

In South Africa, there are some apparent signs of an effort to promote cybersecurity awareness and develop an effective cybersecurity culture (Kritzinger et al., 2017). Despite the global increase in research in cybersecurity globally, there is still a dearth of research on cybersecurity focusing on South Africa (Gwebu et al., 2020). The lack of understanding on the continent about the risks of accessing cyberspace contributes to a permissive climate for cybercrime (Serianu, 2017). Furthermore, the digital infrastructure development level in African countries directly impacts their security posture (Serianu, 2017). According to reports, cybercriminals rely on the general public's poor security practices; thus, policymakers ought to engage in public awareness campaigns due to the fact that there is substantial evidence that such programmes can effectively cut the success rate of cybercrime (Bada, Von Solms et al., 2019). White papers estimate that investing in cybersecurity awareness and training can affect user behaviour and minimise cyber-related risks by 45% to 70% (Bada, von Solms et al., 2019). Unfortunately, current literature and reports show a bleak picture of the increase in cybercrime in Africa,

attributed to the low ICT literacy levels that may hinder cybersecurity awareness efforts (Bada, Von Solms et al., 2019).

2.3 Cybersecurity Vulnerabilities in Universities

Universities are, by nature, open with a dense population and private data, which means that they attract a substantial number of cyberattacks due to a large amount of cyberspace usage (Yusif & Hafeez Baig, 2021). Some of the capabilities universities hold in this age of e-learning include online teaching and learning software, digital libraries, free Wi-Fi, and so on, which increases exposure to cybercrime susceptibility (Ajaero, 2020). Furthermore, universities position themselves at the forefront of technological innovation, opening them up to more vulnerabilities to increased security attacks (Yusif & Hafeez-Baig, 2021). Openness, which makes educational institutions susceptible to cyberattacks and data breaches, is a source of concern, with some scholars reporting that in excess of millions of data breaches are already being experienced by multinational organisations (Chapman, 2019). Still, the exposure of academic data is not as widely publicised (Chapman, 2019). Some scholars argue on the contrary that other industries do not report their breaches, due to a lack of investor confidence, and loss of competitiveness (Grama, 2014).

Vulnerabilities found in universities inferred from literature are classified into a few categories. The first category is administrative and cultural domains, which can clash with cybersecurity requirements. In this category, a lack of awareness and knowledge of cybersecurity best practices significantly affects the implementation of cybersecurity policies and leads to a violation of these policies (Ulven & Wangen, 2021). In addition, poor cybersecurity management can increase the vulnerability of universities to cyberattack, as they are unprepared to deal with an attack when it occurs (Nyblom et al., 2020). The second category is the technical domain, where vulnerabilities are caused due to shortfalls in the technology or systems in place (Ulven & Wangen, 2021). In this category, one aspect that increases the cybersecurity threat is the norm of students and staff bringing their own devices to work via which they connect to the network (Ulven & Wangen, 2021). The risk here is that these private computers may be used to penetrate the university networks, due to a lack of security protection systems on the devices, which increases the vulnerability to attacks on university data (Goni, 2022).

2.4 Cybersecurity Awareness and Behaviour of University Students

University students use technology and the internet for educational purposes and socialising, which became even more prevalent during the pandemic, when social distancing was encouraged (Alqahtani, 2022). As the future of the workforce, the impact of cybersecurity awareness behaviours of university students is particularly significant for society (Cheng & Wang, 2022). This makes students particularly vulnerable to cybercrime threats, as they make up most of the users of the information systems across universities (Taha & Dahabiyeh, 2021).

With the Covid-19 pandemic and online learning, university students always remain connected to the internet, and they do so by using various devices, which increase the danger of cyberattack if they do not remain vigilant about how they handle their online security (Matyokurehwa et al., 2021). Educational institutions are not taking proactive measures to raise awareness among college students about these issues and how to defend themselves from cyberattacks, such as identity theft or ransomware (Moallem, 2019). A significant risk is having a student body with an increased dependence on digital systems and is connected to the free Wi-Fi offered by the University, that is at once unaware of cybersecurity issues (Taha & Dahabiyeh, 2021). No matter the degree of technology and security the in which the institution invests, students remain the weakest link. Their lack of knowledge or ignorance makes them particularly vulnerable to targeted cyberattack (Taha & Dahabiyeh, 2021).

The trends in student awareness of cybersecurity show that students are unaware of the requisite knowledge and understanding of cybersecurity regulations and their practical application (Moallem, 2019). Another essential aspect to note is that a lack of cybersecurity awareness is not due to a lack of knowledge, but due instead to how students apply it in their daily lives (Moallem, 2019). Studies on the behaviour of students with cybersecurity reveal that engagement with cybersecurity issues was not satisfactory, where, if students were more aware of cybersecurity, some of these threats would be eliminated (Potgieter, 2019).

2.5 Human factor and compliance with cybersecurity measures

The human context is frequently regarded as the weakest link between cybersecurity and organisational information, as it is the main target for increasing cybercrimes (Chandarman & Van Niekerk, 2017). This determines the success or failure of the security chain. Scholars have identified individuals as the weakest link in the security chain as they fail to comply with cybersecurity best practices (Khader et al., 2021). According to a recent study, out of 874 cybersecurity incidents that were reported, 68% were caused internally by negligent individuals, 22% by external criminal individuals, and 10% by stolen credentials (Donalds & Osei-Bryson, 2020). The results of this study indicate that individuals' compliance with cybersecurity remains a challenge, and compliance behaviour is necessary to mitigate the risk of cyber incidents (Donalds & Osei-Bryson, 2020). Thus, cybersecurity depends not only on IT professionals, but also on educated users, who are highly aware of and employ cybersecurity best practices (Alsmadi & Zarour, 2018).

End-users of technology continue to break basic cybersecurity regulations, sustaining the cybercrime sector (Kabanda et al., 2018). User behaviour is crucial to mitigating and preventing cybersecurity issues (Taha & Dahabiyeh, 2021). When people are unaware that they are at risk, they often fail to recognise the attacks (Potgieter, 2019). Thus, students need to understand and be aware of cybersecurity threats and how to mitigate them (Potgieter, 2019).

Attacks against digital assets have not stopped and have become more varied and complicated, due to a lack of user cooperation and awareness, which causes many security approaches vulnerable to being misused or misread by users (Yusif & Hafeez-Baig, 2021). Compliance is based on the human component. This entails adhering to specified guidelines that aid in fulfilling predetermined objectives. Because cybersecurity regulations are viewed as guidelines, rather than as rules, the role of the human component in the bulk of cyberattacks or data breaches is emphasised (Yusif & Hafeez-Baig, 2021). Increased information availability has significant positive effects, but when it comes to changing human behaviour, merely presenting the information does not nearly have as much of an impact (Bada, Sasse, et al., 2019).

3 Theoretical Framework

Protection motivation theory (PMT) provides the theoretical framework for this study. PMT focuses on evaluating human behaviour regarding their motivation to respond to threats. The theory has been used in various studies to investigate individuals' protection behaviours.

3.1 Justification for selection of theory

The theory postulates that the past behaviours of an individual affect how they assess threats and their ability to handle them (Vance et al., 2012). Most cyberattacks are attributed to an inadequate level of user cooperation and knowledge. Thus, emphasis on the role of the human factor is being placed

(Van Niekerk & Von Solms, 2010). As a result, PMT was deemed appropriate to investigate the factors that affect the compliance behaviour of university students with cybersecurity measures.

3.2 Protection Motivation Theory (PMT)

PMT has been used in several studies as a tool to understand the motivations for individuals to comply with cybersecurity-related behaviours (Yusif & Hafeez-Baig, 2021). PMT predicts adopting or non-adoption compliance behaviours with cybersecurity (Ezati Rad et al., 2021). The theory has two primary constructs: threat appraisal, and coping appraisal. These two constructs are integrated to develop protection motivation (Ezati Rad et al., 2021). These constructs describe how individuals assess the level of risk they encounter in cyberspace and act as a protective measure (Yusif & Hafeez Baig, 2021). Figure 2. illustrates the conceptual model of the study.

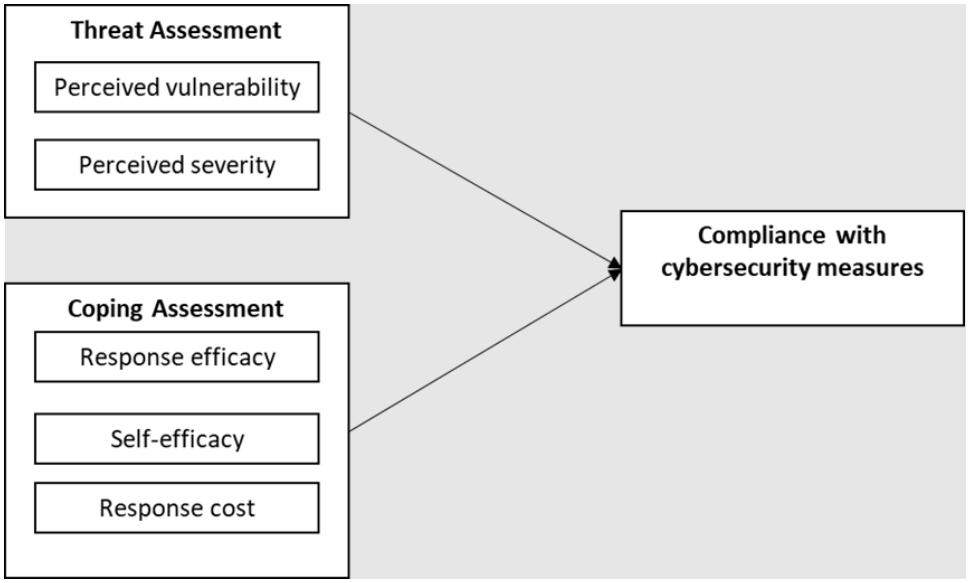

Figure 1: Conceptual model (Adopted from the Protection Motivation Theory (Rogers, 1975))

Threat Assessment

The threat assessment construct focuses on the severity and the evaluation of the threat. It consists of two main components: perceived vulnerability, and perceived severity. *Perceived vulnerability* refers to the individual's appraisal of the likelihood of being exposed to a threat (Rogers, 1975). The theory states that an action taken by an individual to overcome fear is influenced by the probability of its occurrence (Ezati Rad et al., 2021; Towbin, 2019). Therefore, if individuals perceive a low likelihood of the threat occurring, they are less likely to take action.

Perceived severity refers to the extent of the consequences from the threat if it occurs (Ezati Rad et al., 2021; Rogers, 1975; Towbin, 2019). The likelihood that the harm from the threat will have serious repercussions will compel an individual to act against the threat.

Coping Assessment

Coping assessment refers to a person's appraisal of their ability to respond to a threat (Crossler et al., 2019). This construct consists of three components: response efficacy, self-efficacy, and response cost. *Response efficacy* refers to the individual's belief that the recommended action is effective in mitigating the threat (Crossler et al., 2019; Tsai et al., 2016). Self-efficacy refers to an individual's belief in their ability to carry out the recommended action (Crossler et al., 2019). *Response cost* refers to the perceived costs related to conducting the recommended action against a threat or engaging in security behaviours (Crossler et al., 2019; Towbin, 2019), for instance, the costs of using Antispyware.

Overall, previous studies employing PMT show that self-efficacy and response efficacy have a significant relationship with the behavioural intentions of individuals in compliance with cybersecurity (Miraja et al., 2019). The constructs of the PMT used in this study are operationalised in Table 1.

Construct	Definition	Source
Perceived Vulnerability	The extent to which students think they are vulnerable to cyber threats.	Rogers, 1975; Yusif & Hafeez Baig, 2021
Perceived Severity	The degree to which the students perceive the seriousness of the threat/risk if it was to occur.	Rogers, 1975
Response efficacy	The degree to which students believe the recommended cybersecurity actions would help them avoid the threat.	Rogers, 1975; Yusif & Hafeez-Baig, 2021; Crossler et al., 2019
Self-efficacy	The extent to which students believe they can successfully perform the recommended tasks.	Tsai et al., 2016; Crossler et al., 2019
Response Cost	The costs of complying to cybersecurity measures set by the University, and the cost of non-compliance.	Towbin, 2019; Crossler et al., 2019

Table 1: PMT constructs

4 Context of the study

The University of Cape Town (UCT) is one of the top universities in Africa and the world. It is located in the Western Cape province of South Africa (UCT News, 2022). In 2021, it was estimated that the University enrolled over 30 000 students (UCT News, 2022). UCT boasts several advanced technologies to facilitate student learning. To ensure compliance with international ICT standards and guidelines, a secure cyber environment, and the protection of critical information, the University has developed various ICT policies such as an information security policy, account and password policy,

and anti-virus policy (UCT ICTS, 2022). The University also offers ICT services to support academic staff, students, and management on ICT-related matters.

Compliance with ICT policies has always been challenging for many organisations worldwide, including universities. Scholars have pointed to a lack of motivation, awareness, belief, and behaviour as the main contributing human factors in non-compliance (Alqahtani & Braun, 2021; Da Veiga et al., 2020).

5 Research Methodology

We followed an interpretive philosophy to conduct this research. The interpretive stance argues that truth and knowledge are subjective; thus, by adopting an interpretive philosophy, the researcher will be able to understand and interpret the experiences of respondents/subjects of the research (Kivunja & Kuyini, 2017). Adopting an interpretive approach is appropriate for this study, as it allows for a rich understanding of the phenomena and, in this case, an understanding of the factors affecting university students' compliance with cybersecurity measures (Orlikowski & Baroudi, 1991).

The study adopted a deductive approach. In this case, a conceptual model was developed using constructs from the PMT. We utilised a qualitative research approach by employing a case study of UCT. Data was collected using semi-structured interviews and observations of students' engagement with cybersecurity measures at the University. Semi-structured interviews allowed us to interact and fully engage with participants by asking follow-up questions.

The target populations were students and ICT staff at UCT. The students consisted of undergraduate students in different academic years across the University's six faculties. We chose this sample because undergraduate students make up most of the student population, constituting the University's largest users of information systems (UCT News, 2022). In 2021, UCT had 30 329 registered students, with 18 154 undergraduates, where undergraduate students make up more than 59% of the student population.
(UCT News, 2022). This makes undergraduate students the weakest link in the University's cybersecurity chain (Chandarman & Van Niekerk, 2017). We included staff members from ICTS to gain their perspectives as they are part of developing cybersecurity-related policies and interact with students on cybersecurity-related matters such as compliance with the University's ICT policies.

The study employed purposive sampling, a sampling technique where the researcher chooses participants based on personal judgement, and convenience sampling, which are selected participants at the researcher's convenience. The study also incorporates snowball sampling, where the initially chosen participants recruited or recommended more participants to participate. The purposive sampling technique was selected because the researchers were interested in university undergraduate students. Conversely, the convenience sampling method was applied because the researchers could conveniently access the sample. Therefore, the snowball sampling technique was used as purposive sampling could not yield the desired results.

A total of 40 responses were collected, of which 35 were students, while five respondents were staff members from ICTs. The students were coded as Respondent_student_X and the staff Respondent_staff_X. Table 2 summarises the demographic information of the respondents.

Respondents Positions:		
	Undergraduate students	35
	ICT staff	5
Age Range:		
	46 years above	2
	36-45 years	3
	26-35 years	11
	16-25 years	24
Faculty Departments:		
	Faculty of Commerce	13
	Faculty of Humanities	8
	Faculty of Science	6
	Graduate School of Business	3
	Faculty of Law	2
	Faculty of Engineering and Built Environment	3

Table 2: Demographic Information of Respondents

The interviews were recorded and later transcribed for analysis. The interviews lasted between eight and 20 minutes. Data was analysed using thematic analysis and Nvivo software. Collected data was organised and categorised according to themes as per the constructs. The research was conducted in line with the ethical standards of the University of Cape Town. We obtained ethics approval for the study from the University prior to the commencement of data collection.

6 Empirical analysis and Discussion

This section uses PMT to understand the underlying factors affecting students' compliance with cybersecurity measures. The findings and the discussions are further explained in the subsequent sections. Participant responses are cited verbatim.

6.1 Threat Assessment

We were set to understand how threatened the respondents felt about the possibility that they could encounter cyberattacks. In addition, it assisted in determining those factors would likely affect the respondents' decision to not comply with cybersecurity measures set by the University.

Perceived vulnerability

The majority of students did not think they were likely to be targeted by cybercriminals. The reason is that the students believed that they did not have any valuable information for cybercriminals to target.

"I am a student, and personally, I feel I do not have any valuable information that would be useful for the attackers. I think the attackers go for top government officials or high-profile people who may have confidential information. They easily target those because they can demand ransom." [Respondent_Student_4]

Furthermore, the students did not perceive that they were vulnerable, since they were protected by ICT protection measures put in place by the institution. The trust in the university's ICT service was consistent among the students, who believed that the likelihood of being a victim of cyberattacks was low, because ICT service at their University offered them protection. As a consequence, they felt safe even if they did not take additional measures.

"I strongly believe that the University has built adequate infrastructure to protect the students and the staff. So, I believe our University is safe from cyberattacks." [Respondent_student_7]

"As a student, I am less likely to be a victim. Because we have a lot of software, and we have ICT services to help us with ensuring that there's protection from being attacked." [Respondent_student_3]

This finding reflects the broader literature, as many individuals rely on third-party protective measures. They do not believe that the responsibility lies with them (Interpol, 2021; Murphy et al., 2022).

In summary, students did not comply with the cybersecurity measures set out by University's ICT service department because they were not likely to be victims of cyberattacks, due to not owning valuable information and the protection given to them by ICT service at the University. However, when an individual believes that a threat of cybercrime is likely to occur, they are more motivated to comply with cybersecurity measures (Tsai et al., 2016).

Perceived severity of the threat

We asked the respondents to elaborate on the perceived severity if they were victims of cyberattacks. The respondents indicated that they did not perceive the true severity of the security predicament, because they had never encountered any cyberattacks.

"Since I started my studies at this University, I have never encountered any cyberthreats. So, when I browse on my device, I can download anything and do whatever pleases me." [Respondent_student_19]

The students' perception affected their compliance with the cybersecurity measures. These findings are supported by literature, which states that when individuals are unaware of the threats that they face, they are more likely to engage in unsafe behaviour, without taking the necessary protective measures (Potgieter, 2019).

The responses from the students corroborated those of UCT's staff members. The staff members indicated that even though the University's ICT service invited students to cybersecurity awareness events, most students did not attend them.

"Even if we have cybersecurity awareness sessions, students will rarely attend. Students will only really take it seriously once they are compromised. Otherwise, they don't really care until it happens to them; that's when they wake up and realise how important it is." [Respondent_staff_2]

The non-compliance of students with the basic cybersecurity measures set out by University's ICT service can be linked to them not feeling threatened by the cyberattack. As such, most of these students did not implement any cybersecurity measures, for instance, an anti-virus mechanism. The ICT anti-virus policy of the University stipulates that all computers in the university environment need to have

an anti-virus mechanism installed to protect the computers from viruses and other malicious code. However, when we enquired from the staff members as to whether they had implemented incentives to promote cybersecurity compliance in the University, they did not have any mechanisms in place.

> *"I honestly don't remember installing any anti-virus. The only cybersecurity measure I have installed is the authenticator, which the University's ICT service had put mandatory measures for me to continue using the UCT applications."* [Respondent_student_30]

On the other hand, although some students did not perceive the severity of cybercrimes, they took personal protective measures against cyberattacks. The students indicated that they installed multi-step authentication and anti-virus applications on their devices. The students emphasised that they found the severity of the threat of becoming a victim of identity theft high, in response to which they took precautions. The students related their protective actions to the fear of their devices being compromised.

> *"I'm paranoid of identity theft. So, I make sure I install and update my anti-virus regularly. Everything associated with my personal information, I protect at any cost."* [Respondent_student_14]

This finding is supported by the literature, which states that when individuals feel threatened by cybercrime, they are more motivated to comply with cybersecurity measures to remove the threat (Towbin, 2019).

6.2 Coping Assessment

Response Efficacy

Most of the students in the study knew what they had to do to protect themselves. When asked about which protective measures they thought students ought to take, their responses were similar as they based these on the measures set by University's ICT service. The respondents believed that taking these actions would help them avoid the threat of cyberattacks.

> *"make sure that your anti-virus software is always up to date? Make sure you go there and try CTS and have it installed if you don't understand. Make sure that you don't visit any of those illegal sites for movies for series. Rather install Netflix if you can't afford one, then I don't know man, but just don't visit those illegal movie sides and follow one to make a feature."* [Respondent_student_23].

On the other hand, although some students knew about the various protective measures, they did not believe they were necessary to implement them.

> *"I don't think you need some anti-virus or ever. I think what's on your computer already is enough."* [Respondent_student_5].

An individual's belief that the recommended protective action would help them avoid the threat motivates them to take action (Yusif & Hafeez-Baig, 2021). However, when an individual believes that installing anti-virus software on the device does not offer them any protection, they will not be motivated to install it, even if that is the recommended action to take. This matches what was found in the research, as students responded that they did not think installing anti-virus software would be necessary, so they did not install it, even though that does not comply with University's ICTs anti-virus policy.

Self-efficacy

The students had lower self-efficacy in terms of their ability to protect themselves. They believed that they had to have the technical skills to be able to protect themselves. This could have made them rely on ICT services in the institution. Even when they were aware of the risks, they did not initiate and were lenient in their protective measures.

"So students are normally very lenient, in the sense that they don't take note much of things. So there are plenty of security measures and tips to prevent cyber tech from happening, but students tend to ignore them. Students don't like reading notifications and things like that." [Respondent_staff_24]

The response from the staff member showed that, even though students had the knowledge and awareness of cybersecurity, they were still lenient in complying with cybersecurity measures, as they did not believe they were responsible for their safety on the internet.

The respondent's lack of ability to protect themselves could have been attributed to the lack of engagement with cybersecurity issues, for instance, cybersecurity awareness. The study revealed that cybersecurity awareness is crucial to students' compliance with cybersecurity measures.

Many students had little to no engagement with cybersecurity as they had no knowledge of it. However, responses from students also showed that few amongst those students who were more interested in cybersecurity were in fact actively engaged with it. The students stated that they conducted research and read emails sent by University's ICT service. This made them more aware of the risks and motivated them to protect themselves against potential cyberattacks. This finding indicated that cybersecurity awareness was largely missing in the institution, which counteracted the responses from the staff members.

"The only cybersecurity awareness event I attended was during my first year. The UCT department gave a security talk to the students who were on financial aid. I believe they are more focused on those students because the students are given university laptops." [Respondent_student_9]

Response Cost

The cost of complying was one of primary reasons why students did not comply with cybersecurity measures. Students cited that taking protective measures takes time, effort, and financial resources. The findings show that the higher the cost of compliance, the lower the motivation to comply with cybersecurity measures.

"Honestly, for you to install the software and also make sure they are updated, costs a lot of time and effort. In addition, I need to always have WIFI available to ensure that I update my devices." [Respondent_student_8]

When the cost of compliance is higher than they are willing and able to pay, an individual is less motivated to comply (Alqahtani, 2022; Alqahtani & Braun, 2021). The finding is consistent with the existing literature.

When it comes to the cost of non-compliance, the students felt that in the case of an attack they would likely lose some information. However, they believed that they did not harbour the kind of information that thieves would likely be interested to steal. Consequently, the respondents believed that the cost of non-compliance was low.

"Personally, nothing. When I think about it, I only have pictures, So I don't even mind in my opinion. Okay." [Respondent_student_11]

Furthermore, the study found that since the University did not have mechanisms to penalise students for non-compliance with cybersecurity measures, this reduced the perceived cost of non-compliance. A high cost for non-compliance may nudge individuals towards it (Towbin, 2019).

7 Conclusion and Recommendations

The study sought to understand the factors affecting university students in South Africa in complying with cybersecurity measures. The research adds to a body of literature to understand the underlying factors affecting compliance by students in developing countries. The study found that the perceptions of students regarding the severity of the threat, the likelihood of the threat to occur, their lack of belief in the cybersecurity measures in place and the cost associated with compliance affected cybersecurity compliance by students. In addition, a lack of cybersecurity awareness and knowledge may have contributed to compliance. Therefore, universities needed to create targeted cybersecurity awareness-raising initiatives. In addition, the University ought to implement metrics to measure the effectiveness of those cybersecurity awareness initiatives currently in place. Furthermore, universities ought to create incentives to promote cybersecurity compliance. This could be achieved through the hosting of competitions, along with sponsorships for cybersecurity seminars to motivate students' compliance and create awareness.

The sample was drawn from one University in South Africa, which may have limited the findings, and the generalisability of the study. Therefore, we recommend future research drawing from across a range of universities in South Africa.

References

Ajaero, C. C. (2020). *Behavioral characteristics computer users need to minimise ransomware exposure* (Publication No. 28149194) [Doctoral dissertation, Capella University]. ProQuest Dissertations & Theses Global.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2). https://doi.org/10.3390/bdcc5020023

Al-Moshaigeh, A., Dickins, D., & Higgs, J. L. (2019). cybersecurity risks and controls. *The CPA Journal*, *89*(6), 36–41.

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

Alqahtani, M.A., & Braun, R. (2021). *Examining the Impact of Technical Controls, Accountability and Monitoring towards Cyber Security Compliance in E-government Organisations*. https://doi.org/10.21203/rs.3.rs-196216/v1

Alsmadi, I., & Zarour, M. (2018, August 20). Cybersecurity Programs in Saudi Arabia: Issues and Recommendations. *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*. https://doi.org/10.1109/CAIS.2018.8442013

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

Bada, M., von Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness in Africa: An Empirical Study: an empirical study. *The Third International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2018,* 78-83

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24-31.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, *20*, 133–155.

Chapman, J. (2019). How safe is your data? Cyber-security in higher education (Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute.

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information (Switzerland)*, *13*(4). https://doi.org/10.3390/info13040192

Crossler, R. E., Andoh-Baidoo, F. K., & Menard, P. (2019). Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of U.S. and Ghana. *Information and Management*, *56*(5), 754–766. https://doi.org/10.1016/j.im.2018.11.009

da Veiga, A., Astakhova, L. v., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers and Security*, *92*. https://doi.org/10.1016/j.cose.2020.101713

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

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin*, *46*(1), 78–109.

Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is it possible to change the cyber security behaviours of employees? Barriers and promoters. *Academic Journal of Interdisciplinary Studies*, *10*(4), 210–224. https://doi.org/10.36941/AJIS-2021-0111

Ezati Rad, R., Mohseni, S., Kamalzadeh Takhti, H., Hassani Azad, M., Shahabi, N., Aghamolaei, T., & Norozian, F. (2021). Application of the protection motivation theory for predicting COVID-19 preventive behaviors in Hormozgan, Iran: a cross-sectional study. *BMC Public Health*, *21*(1), 466. https://doi.org/10.1186/s12889-021-10500-w

Goni, O. (2022). Introduction to Cyber Crime. *International Journal of Engineering and Artificial Intelligence*, *3*(1), 9–23. https://doi.org/10.55923/jo.ijeal.3.1.701

Grama, J. L. (2014). *Legal Issues in Information Security: Print Bundle*. Jones & Bartlett Publishers.

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy non-compliance: An integrative social influence model. *Information Systems Journal*, *30*(2), 220–269. https://doi.org/10.1111/isj.12257

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 817-885.

Hubbard, J. (2019). SA business underplaying the danger of cybercrime. *Finweek*, *2019*(4), 37–38. www.thecyberacademy.co.za

Interpol. (2021). *African Cyberthreat Assessment Report*. Retrieved, December 19, 2022 from https://www.interpol.int/en/content/download/16759/file/AfricanCyberthreatAssessment_English.pdf

Jeyaraj, A., & Zadeh, A. (2020). Institutional Isomorphism in Organizational Cybersecurity: A Text Analytics Approach. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 361–380. https://doi.org/10.1080/10919392.2020.1776033

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information (Switzerland)*, *12*(10). https://doi.org/10.3390/info12100417

Kivunja, C., & Kuyini, A. B. (2017). Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education*, *6*(5), 26–41.

Kritzinger, E., Bada, M., & Nurse, J. R. C. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. *IFIP World Conference on Information Security Education*, 110–120.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

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

Lukehart, A. (2022, July 5). *Top 5 Cybersecurity Threats Facing Higher Education*. Fierce Education. https://www.fierceeducation.com/technology/top-5-cybersecurity-threats-facing-highereducation

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Chipfumbu-Kangara, C. (2022). Enhanced social engineering framework mitigating against social engineering attacks in higher education. *Security and Privacy, 5*(5), e237.

Mlambo, C. (2021). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and Privacy*, *4*(2). https://doi.org/10.1002/spy2.141

Miraja, B. A., Persada, S. F., Prasetyo, Y. T., Belgiawan, P. F., & Redi, A. A. N. P. (2019). Applying protection motivation theory to understand Generation Z students intention to comply with educational software anti-piracy law. *International Journal of Emerging Technologies in Learning*, *14*(18), 39–52. https://doi.org/10.3991/ijet.v14i18.10973

Moallem, A. (2019). *Cybersecurity Awareness Among Students and Faculty* (1st ed.). CRC Press. https://doi.org/10.1201/97804

Morgan, H. (2020). Best Practices for Implementing Remote Learning during a Pandemic. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, *93*(3), 135–141. https://doi.org/10.1080/00098655.2020.1751480

Murphy, C., Mtegha, C. Q., Chigona, W., & Tuyeni, T. T. (2022). Factors Affecting Compliance with the National Cybersecurity Policy by SMMEs in South Africa. *African Conference on Information Systems*. https://digitalcommons.kennesaw.edu/acist/2022/presentations/4

Nyblom, P., Wangen, G. B., Kianpour, M., Østby, G., & Wangen, G. (2020). The Root Causes of Compromised Accounts at the University. *ICISSP*, 540–551. https://www.researchgate.net/publication/334226938

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organisations: Research Approaches and Assumptions. *Information systems research, 2*(1), 1-28. https://www.jstor.org/stable/23010611

Potgieter, P. (2019). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. *ICICIS*, 272–280.

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

Serianu. (2017). *Demystifying Africa's Cyber Security Poverty Line*. https://serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, *26*(2), 1721–1736. https://doi.org/10.1007/s10639-020-10330-0

Towbin, R. S. (2019). *A protection motivation theory approach to healthcare cybersecurity: A multiple case study* [Doctoral dissertation]. Northcentral University.

Traxler, J., Smith, M., Scott, H., & Hayes, S. (2020). *Learning through the crisis: Helping decisionmakers around the world use digital technology to combat the educational challenges produced by the current COVID-19 pandemic*. https://wlv.openrepository.com/bitstream/handle/2436/623926/Traxler_et_al_Learning_through_the_crisis_2020.pdf?sequence=3

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 and Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

UCT ICTS. (2022). *Policies and guidelines*. https://www.icts.uct.ac.za/about-icts/policies-andguidelines

UCT News. (2022). *About UCT and Cape Town*. https://www.news.uct.ac.za/article/-2022-02-09about-uct-and-cape-town

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. In *Future Internet* (Vol. 13, Issue 2, pp. 1–40). MDPI AG. https://doi.org/10.3390/fi13020039

van Niekerk, J. F., & von Solms, R. (2010). Information security culture: A management perspective. *Computers and Security, 29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where?. *Information & Computer Security, 26*(1), 2-9.

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

Yusif, S., & Hafeez-Baig, A. (2021). Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework. *Journal of Applied Security Research*. https://doi.org/10.1080/19361610.2021.1989271