Issues in Information Systems
Volume 24, Issue 4, pp. 294-310, 2023

DOI: https://doi.org/10.48009/4_iis_2023_123

The impact of technostress creators on academics' cybersecurity fatigue in South Africa

John Mangundu, *University of the Witwatersrand, john.mangundu@wits.ac.za*
Thembekile Mayayise, *University of the Witwatersrand, thembekile.mayayise@wits.ac.za*

Abstract

The intention of this study is to examine from a behavioral perspective, how technostress impacts on academics' cybersecurity compliance in universities where the protection of information systems has become of vital importance due to increased dependency for academic business. The authors proposed a research framework informed by the Technostress Creators' Model and the Theory of Planned Behavior that cybersecurity fatigue moderates compliance intention. Data collected through a closed ended online survey questionnaire from 210 academics in one public university in South Africa was analyzed using descriptive statistics and the proposed model was evaluated through partial least squares structural equation modeling (PLS-SEM). The results from empirical investigation reveal that technostress creators of techno-complexity, techno-invasion and techno-insecurity positively influence cybersecurity fatigue. However, techno-uncertainty and techno-overload demonstrated a negative influence on cybersecurity fatigue. Furthermore, results revealed moderation of cybersecurity training and awareness on cybersecurity fatigue. This paper aims to improve cybersecurity compliance by academics in universities by understanding the effect of technostress and cyber fatigue on cybersecurity compliance behavior. The study is of significance to universities management, especially academics information communication technologies skills development and workload administration, as they are informed on how to better develop initiatives and strategies for improved cybersecurity compliance.

Keywords: technostress, fatigue, cybersecurity compliance behavior, higher education, South Africa.

Introduction

Higher education institutions have become more reliant on information systems for managing administrative, research and academic processes, involving personal data, and have become attractive targets for cyber-criminals and hackers (FireEye, 2016). Incidents of higher education institutions having been severely hurt from such attacks (Garrison, 2010; Bongiovanni, 2019), have been reported in the higher education environment. The need for information security in higher education spaces has been on the rise in the last decade. This has been necessitated by the increase in threats and risks, leading to serious data breaches in instances of improper cybersecurity compliance behavior. To protect critical information assets, institutions have adopted complex cybersecurity mechanisms, as part of the security solutions (Ifinedo, 2014), either through technical or a combination of technical and non-technical mechanisms to protect their information assets. Studies reveal the existence of different technical security mechanisms, for example Wang and Jones (2020) revealed the significance of spam email detection through hidden Markov model (HMM) based data analytics, Suhag and Daniel (2023) revealed that statistical and artificial intelligence based distributed denial of service (DDoS) defensive solutions were effective in curbing against DDoS attacks. The sophisticated technical tools by themselves, prove to be inadequately providing protection (Li

et al., 2019). In contrast, institutions implementing a combination of the measures (Herath & Rao, 2009a), improve their likelihood of success in protecting their information assets (Stanton et al., 2005; Pahnila et al., 2007), as the non-technical measures are targeted at improving individuals' cybersecurity compliance behavior.

Despite different organisational initiatives to advance cybersecurity compliance, literature reveals internal individuals as the major players in intentional and unintentional security incidents (Donalds & Osei-Bryson, 2020; Barlow et al., 2013). Some individuals do not give these security policies serious considerations. Despite their availability, individuals in institutions are failing to completely comply with security policies (D'Arcy & Lowry, 2019; Siponen et al., 2014), proving that security policies are not guaranteed to work effectively for individuals (Li et al., 2019; Han et al., 2017). Given the significant importance of individuals' involvement in improving security, institutions also embarked on cybersecurity training and awareness programmes for their employees (Telstra Corporation, 2018), with the aim of educating individuals about acceptable cybersecurity compliance behavior, and consequences of non-compliance (D'Arcy et al., 2009).

Scholars and practitioners have accepted the importance of individuals in attaining security, and individuals having been pronounced as the main sources of security vulnerabilities as they fail to satisfy requirements for security best practices (Warkentin & Willison, 2009; Yeniman et al., 2011). However, evidence demonstrate that there seem to be an absence of a strong connection between level of individuals' cybersecurity training and their cybersecurity compliance (Pattinson et al., 2016b; Parsons et al., 2013). Individuals who have received more than adequate security training from their institutions do not necessarily display advanced levels of cybersecurity compliance behavior (Ng & Xu. 2007). Resultantly, internal individuals' security compliance behavior became a crucial management subject in organisations, as well as an important topic of research consideration by scholars (Donalds & Osei-Bryson, 2020). Support is given by cybersecurity insiders (2018), who reported that an excess of 90% cybersecurity practitioners believe that institutions are more exposed to cybersecurity threats from internal individuals. These arguments demonstrate the persistent problems associated with individuals' compliance behavior in relation to cybersecurity.

Despite previous scholars having studied the relationship between technostress and traditional business workplace behaviors (Atanasoff & Venable, 2017; Ayyagari, 2008; Tarafdar et al., 2010, 2015), few studies had concentrated on the phenomenon in relation to cybersecurity fatigue by academics in higher education contexts that recently emergently implemented ICTs. Other scholars have recently extended the technostress phenomenon to social media use (e.g., Maier et al., 2015; Salo et al., 2019). Through contextualization of the technostress phenomenon in the higher education environment, the current study extends technostress to a unique context. As advocated by Hong et al (2014), contextualization of empirical research is vitally important for advancing contextually relevant technologies. In addition, to the researcher's knowledge, very few studies have characterized the moderating effect of intervention strategies (cybersecurity training and awareness and cybersecurity monitoring) on these direct relationships, which the current study seeks to determine. Overall, the study seeks to answer the following questions.

Research questions

1) *What is the impact of technostress creators on cybersecurity fatigue?*
2) *How does cybersecurity monitoring, training and awareness moderate the relationship between techno stressors and cybersecurity fatigue?*
3) *How does cybersecurity fatigue relate to cybersecurity compliance intention?*

South African cybersecurity policies

Online privacy and security are becoming more and more regulated in South Africa. The Electronic Communications and Transactions Act (ECT) of 2002 is the founding statute from which all subsequent legislation is derived (RSA, 2002). Also adopted in 2002 was the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) (RSA, 2002). Published in 2009 and passed in 2013 (RSA, 2009; RSA, 2013), the Protection of Personal Information (POPI) Bill has fully taken effect. The POPI act in now in act, hence organisations are required to comply with the act. However, there are loopholes with some companies failing to comply. Limitations exist from the government as the regulator to ensure oversight and compliance enforcement through penalties. The end of 2015 saw the publication of the National Cybersecurity Policy Framework (SSA, 2015), and the Cybercrimes and Cybersecurity Bill drafts (Department of Justice and Correctional Services, 2017). However, despite various cyber policies having been designed, it has been stated that over half a billion online personal records were lost or illegally accessed in South Africa during 2015, and that South Africa lost around ZAR50 billion in 2014 because of cyber-incidents (SABC News, 2017). The financial damages from cyberattacks were estimated to reach ZAR 3.7 billion in direct losses and ZAR 6.5 billion in indirect expenditures in 2011(Norton South Africa, 2012). The threat will extend more widely in future as South African internet usage rises, helped by the continent of Africa's expanding undersea capacity (Song, 2017). Against this backdrop, the current study focuses on the behavioral intention to comply with cybersecurity requirements by academics in a South African university, as further contextualized in the succeeding section.

Contextualization and significance of the study

In actuality, the study focuses on a South African university community represented by academic staff and this community provides participants from various regions of South Africa and reflect a variety of "races, cultures, languages, and beliefs." According to Hofstede, these background variations are also likely to affect how each person behaves (1984). Likewise, Buchtel et al. (2015) and Sang et al. (2015) separately reaffirmed that cultural differences affect how people perceive and behave, which affects what is socially acceptable or unacceptable conduct. The variety in the university employees is furthered by the variations in their educational backgrounds and cultural variances. Most participants in the current study come from historically underserved South African townships and rural areas, with limited access to ICTs throughout their educational and developmental journeys. Recent employment laws are conscious of racial, gender, and ethnic diversity and aim to give people who passed through the above-mentioned defective educational system equitable chances. As a result, people are now in settings where they must adopt pedagogical advances supported by technology that come with requirements such as cybersecurity compliance. Therefore, it can be assumed that the study sample consists of a mix of participants who are digitally proficient, digitally incompetent, digital immigrants, and digital natives. These participants may offer interesting, contextually informed responses that are informed by the participants' backgrounds.

Considering the above, the researchers contend that, for the most part, it is the context that makes it unpredictable, difficult, and potentially challenging to realize the users' behavioral intentions to comply with cybersecurity expectations. Due to the differences in their educational and cultural backgrounds, which also influence their levels of technostress tolerance, cyber fatigue, and intention to comply with cybersecurity regulations, the respondents from the university provide the right mix expected to offer a lively insight on the phenomena under investigation. The diversity of answers may also allow for intriguing research on the results of cybersecurity enhancement measures such as monitoring, training, and awareness campaigns. By examining the impact of technostress on lecturers' cyber fatigue and how cybersecurity initiatives moderate the relationship, this study aims to contribute to the conversation on cybersecurity in the HE environment. It is argued that the study is important because, once the technological stress factors

that affect lecturers' cybersecurity compliance behavior in this context are known, recommendations and efforts can be made to address them and advance cybersecurity compliance in higher education environments, as well as possibly other related contexts. The literature on cybersecurity is discussed in the section that follows.

Literature review

Studies (Bulgurcu et al., 2010; D'Arcy et al., 2014; Whang et al., 2017) reveal that cybersecurity compliance levels decrease as individuals view the need for compliance as additional responsibilities (time and effort) and is stressful. Individuals could be overwhelmed and tired from the stresses of using technology to execute their roles and functions, consequently leading to disengagement from cybersecurity behavior (Furnell and Thomson, 2009). In addition, employees might feel that security compliance requirements are difficult to comprehend, threatening, and misaligned with their main job roles (Stanton & Stam, 2008; Puhakainen & Siponen, 2010; Posey et al., 2014). This study argues that a possible reason for the non-correlation between intensity of cybersecurity training and the anticipated cybersecurity behavior could be that employees are suffering from technostress. This is especially true during the periods of emergent remote teaching (ERT), where academics suddenly found themselves being required to acclimatize with various information communication technologies (ICTs) for teaching, learning, research and community engagement. Technostress is stress experienced by individuals in workspaces, emanating from information technology use (Ragu-Nathan et al., 2008; Ahmad, 2012), as they are the most regularly used technologies at work, and the continuous connectivity and availability that leads to distorted work-home life boundaries (Tarafdar et al., 2010). In most situations, technostress stems from the mandatory use of technology, when the job requirements mismatch individuals' technological competences, resources, knowledge, skills and needs, which may lead to performance anxiety (Clute, 1998).

Several studies have examined the manifestation of technostress, the causal effect of technostress creators to individual behavior, and distinguished theoretical contributions have been made accordingly (Brillhart, 2004; Tarafdar et al., 2007). Four forms of technostress thus, data smog, multitasking madness, computer hassles, and burnout were identified by Brillhart (2004). Data smog pertains to information load, that has the potential for information fatigue. Multitasking madness is concerned with the multitasking abilities of computers and restricting individuals' mind capabilities. Computer hassles pertain to the annoyances that is caused by ICT (such as pop-up adverts, malware, etc.). Lastly, burnout which is associated with exhaustion emanating from increased pressure and decreased satisfaction from ICT use. Individuals get stressed from the technostress creators such as techno-invasion, techno-overload, techno-uncertainty, and techno-insecurity (Tarafdar et al., 2007; Ragu-Nathan et al., 2008; Fenner & Renn, 2010; Grant et al., 2013). The work of (Brillhart 2004; Tarafdar et al., 2007; Ragu-Nathan et al., 2008), provides a strong theoretical foundation for research on technostress creators and their associated influence on individual behavior in organisations. The sudden shift to online teaching during ERT, resulted in the unexpected increase in sustained effort required of individuals in using technologies on their job roles and individuals, potentially leading to fatigue, anxiousness, exhaustion, and low self-efficacy (Salanova et al., 2014) in using technologies. Resultantly, academics may have become distant, detached, and discouraged from technology and technology related issues such as cybersecurity compliance. Therefore, by interrogating the technostress creators (Tarafdar et al., 2007) model, the study explores the question *"How does technostress creators affect individuals' cybersecurity compliance behavior?"*

Theoretical foundation and hypothesis generation

Various models for studying individual cybersecurity compliance have been developed and tested by scholars and practitioners. These includes the protection motivation theory (Safa et al., 2015; Li et al.,

2019), neutralisation theory (Barlow et al., 2013), theory of planned behavior (Ifinedo, 2014; Moody et al., 2018), general deterrence theory (Chen et al., 2012; Moody et al., 2018) and the rational choice theory (Hu et al., 2010; Vance et al., 2012). These models provide a strong foundation for comprehending motivation behind individual behavior and suggestions for behavior improvement. However, these models mainly take "perceived behaviors", "subjective norms", "perceived rewards", "social influence", "perceived effectiveness", and "perceived susceptibility" as influencers to individual behavior (Lu & Da Xu, 2019; Donalds & Osei-Bryson, 2020) and not technostress creators as factors that may also explain individual cybersecurity behavior.

According to Donalds & Osei-Bryson (2020), the research question of what other factor(s) potentially impact individual cybersecurity compliance becomes inexhaustible. This is supported by Warkentin and Willison (2009) earlier propositions that new ways of understanding individuals' motivations are necessary, through new theoretical foundations. This study responds to the call by integrating a new theory, thus examining the interplay of technostress creators on individuals' cybersecurity compliance behavior. To address the research gap, the study presents and examines the technostress creators (Tarafdar et al., 2007) model, which emphasises technostress from using technology in organisations. The study therefore seeks to empirically validate the assertations by Tarafdar's model to identify statistically significant correlations that may be prevalent between individuals' stress emanating from technology use and their associated cybersecurity compliance behavior.

Technostress creators

Technostress creators involves institutional stressors that produce stress in individuals and are associated with use of ICT (Tarafdar et al., 2007; Ayygari et al., 2011; Srivastava et al., 2015). Techno-invasion (involves technology potentially taking over individuals' lives), techno-overload (pertains to increased work rate and workload), techno-uncertainty (linked to changes in versions of technology used together with associated expectations to the changes), and techno-insecurity (associated with individuals fearing their roles will be taken by other individuals with better technical skills and knowledge) Lastly, techno-complexity (the difficulty of using technologies that drives individuals to feel incompetent). Technostress is normally linked to individuals' duties and responsibilities and the tasks the concerned individuals are expected to perform using technology (Tarafdar et al., 2007), which may result in individuals' failure to copy with the technological demands (Brod, 1984). These stressors proved to increase stress levels within individuals (Tarafdar et al., 2007; Ayygari et al., 2011; Tarafdar et al., 2015).

Individuals' stress is a potential source of organisational non-commitment (Tziner et al., 2015), and other negative behaviors. New or perplexing technological innovations can be a source of employees' stress and result in negative attitude towards the innovation (Atanasoff & Venable, 2017). According to numerous employees' perceptions, the cybersecurity technology systems at their places of employment are making their life more difficult (Calic et al., 2016; Stanton et al., 2016), which will raise their levels of technostress and increase their risk of fatigue. Therefore, in line with D'Arcy et al. (2014), it is likely that technostress emanating from the demands of emergently adopted and complex information communication technologies may have led to increased academics' cybersecurity fatigue. Therefore, the study hypothesises that: -

H1*: Techno-overload is positively related to cybersecurity fatigue.*
H2*: Techno-invasion is positively related to cybersecurity fatigue.*
H3*: Techno-complexity is positively related to cybersecurity fatigue.*
H4*: Techno-insecurity is positively related to cybersecurity fatigue.*
H5*: Techno-uncertainty is positively related to cybersecurity fatigue.*

Cybersecurity monitoring

Cybersecurity monitoring involves the use of technical controls, mechanisms and procedures to compel employees' compliance with cybersecurity policies and procedures (Donalds & Osei-Bryson, 2020). This can be enforced through security policies enforcing what individuals can do or not. However, such enforcements may lead to deliberate disobedience (Reeves, 2021), due to perceived loss of personal control and decision-making (Brehm, 1966; Reeves, 2021). Individuals' behavioral restrictions and monitoring may have detrimental effects as it can upsurge malicious employee behavior (Posey et al., 2011). Hickman et al. (2018) reported that greater cognitive load emanating from cybersecurity monitoring initiatives may result in depletion and habituation of warning messages. Accordingly, Lowry and Moody (2015) proposed for less stringent monitoring mechanisms to increase compliance and reduce the attitudinal type of fatigue (Reeves et al., 2021). Given the provision of institutional initiatives of cybersecurity monitoring, such may possess the potential to moderate the effect of technostress on academics' cybersecurity fatigue. Therefore, the study hypothesises that: -

H7*: Cybersecurity monitoring moderates the relationship between techno stressors and cybersecurity fatigue.*

Cybersecurity training and awareness

In addition to monitoring, institutional cybersecurity training and awareness initiatives are provided. Such initiatives aim at educating employees on acceptable cybersecurity behaviors and the consequences of noncompliance (D'Arcy et al., 2009). However, Pattinson et al., (2016b) reiterated that the relationship between the extent of cybersecurity training and associated compliance is unparalleled and, in some cases, negative. A study by Pattinson et al. (2016b) demonstrated that individuals who were trained on cybersecurity were less aware of cybersecurity in comparison to others. Furthermore, in terms of awareness, individuals may encounter difficulties in managing the massive information and communication from security professionals leading to fatigue (Lee et al., 2016), which may lead to frustration (Zhang et al., 2016). The opposite may be true because properly managed information and communication may lower fatigue and frustration, which are denoted to be individuals' feelings driven by subjective experiences. As such, this study posits that training and awareness may have the potential to moderate the relationship between individuals' technostress and cybersecurity fatigue. Therefore, the study hypothesises that: -

H8*: Cybersecurity training and awareness moderates the relationship between techno stressors and cybersecurity compliance intention.*

Cybersecurity Fatigue

Cybersecurity fatigue denotes a situation where individuals become overwhelmed, tired and frustrated from work pressures and stresses thereby becoming careless in their day-to-day security-related behaviors (Stanton et al., 2016; Reeves et al., 2021). Resultantly, individuals no longer engage with cybersecurity protocols and advice (D'Arcy et al., 2014; Choi & Jung, 2018). Therefore, the study further hypothesises that: -

H9*: Cybersecurity fatigue is significantly negatively related to cybersecurity compliance intention.*

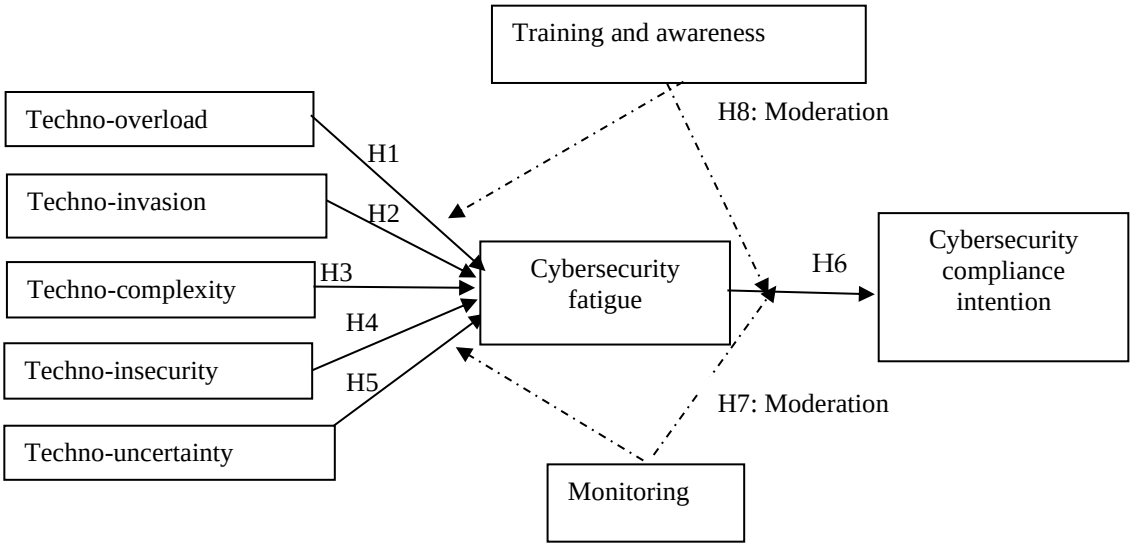

Figure 1: The proposed research framework, adapted and expanded from Tarafdar et al., 2007.

Research methodology

Research methodology is an essential part of a scientific enquiry; it produces reliable results and, as a result, helps to accomplish the study's goal (Henson et al. 2020). The methodology outlines the conditions for data collection and analysis, to answer the research questions and achieve the study objectives.

Questionnaire constructs operationalisation

All the research variables (techno-overload, techno-invasion, techno-complexity, techno-insecurity, techno-uncertainty, cybersecurity fatigue, training and awareness, monitoring and cybersecurity compliance intention) were measured on a five-point Likert scale. Techno stressors were adapted from (Tarafdar et al., 2011) by developing and customizing them to suit the cybersecurity context. Techno-overload was measured with four items, which probed the extent to which respondents perceived stress from the need to work faster and longer. Techno-invasion was evaluated with four items regarding the respondents' perception of stress emanating from being constantly connected and available on online platforms. Techno-complexity was assessed with four items regarding the respondents' perceived inadequacy on their technological skills and knowledge. Techno-insecurity was measured with four items regarding to the respondents' perception of stress emanating from the possible threat of being redundant. Techno-uncertainty was evaluated with four items regarding the respondents' perception of stress emanating from the pace of technological change. Training and awareness were measured with three items concerning the perceived effect of cybersecurity information communication and skilling initiatives. Monitoring was assessed with three items interrogating the perceived effect of cybersecurity control mechanisms in place. Cybersecurity fatigue was measured with four items pertaining to respondents' perceived exhaustion from cybersecurity issues. Construct items on cybersecurity compliance intention were adapted from Vance et al. (2012), Davinson and Sillence (2010), and Ng et al. (2009).Theywere measured with four items enquiring respondents' willingness to observe and abide by cybersecurity demands.

Data collection procedures

The current quantitative study's usage of an online survey questionnaire to gather data from a stratified sample selected from 6 stratum was based on the positivist research paradigm (Andrade 2019).The random method was then used to choose 50 academics from six faculties within the study institution. As a result, 300 academics were targeted as the study's sample and a link to an online survey questionnaire was sent to the respondents (university academics). The online survey questionnaire was setup in SurveyMonkey, with all question items made compulsory to eliminate incomplete responses. Resultantly, the collected number of valid and completed questionnaire responses was 210, demonstrating a response rate of 70%.

Data analysis procedures

Data analysis was conducted using SPSS version 21 to analyze the respondents' demographic data. In addition, SmartPLS version 4 software package was used for partial least squares structural equation modelling (PLS-SEM) (Ringle et al., 2015) in the current study. PLS-SEM is ideal and has been widely used for research in information systems (Hair et al., 2017; Gefen et al., 2011; Ringle et al., 2012).

Results

Descriptive statistics

When analyzing the demographics, the results show most of the respondents were academics who are at lecturer's level (55.2%). Furthermore, the results show that most of the participants (90.8%) have more than four years of experience in academia. Interestingly, despite having 86.1% revealing that they spent more than 6 hours per day on online platforms, 42% indicated that they had less than 3 years of effective ICT use in conducting academic business. Furthermore, demographics demonstrate that most participants (61.3%) perceived themselves as not possessing the adequate skills needed for cybersecurity compliance.

Measurement model assessment

The correlation between the latent variables and their items is explained by the measurement model (Hair Jr et al., 2017). The convergent and discriminant validity of the measurement model must be evaluated to establish its accuracy (Hair Jr et al., 2021). While discriminant validity evaluates how much a latent variable differs from another, convergent validity evaluates how closely connected the indicators of the same latent variable are to one another (Hair Jr et al., 2021).

Factor loadings and convergent validity

The evaluation of the average variance explained (AVE) and the loadings of the items (indicators) is the first stage in determining the validity of the measurement model. According to Hair et al., the loadings should be within the range of the threshold, 0.7 or above, and the AVE for all constructs should be 0.5 or above (2017). It is important to note that, as stated by Hair et al., loadings between 0.4 and 0.7 are only taken into account for deletion if doing so results in an increase in composite reliability (CR) and AVE (2017). Results reveal that there are no problems with convergent validity since all indicators have loadings that are greater than or equal to 0.7, which is the suggested cutoff. The AVE is then measured against a threshold of 0.5. Results indicate that AVE values for all constructions fall within the acceptable range of 0.5 to 0.8. Additionally, the range of rho A is between 0.7 and 0.9, which is within the bounds of the suggested value of 0.7. (Latan et al., 2018). Convergent validity is proven by exceeding the AVE and item loading thresholds (Hair et al., 2017).

Testing internal consistency and reliability is the second step in the measurement evaluation process. In exploratory research, like the current study (Hair et al., 2017), CR can be in the range of 0.6 to 0.7, and Cronbach's alpha is preferred to be above 0.7. The CR results agree with the crucial values when the range of values (0.8-0.9) is greater than the threshold. The Cronbach's alpha is then compared to the threshold. The obtained value range (0.7-0.9) is within the suggested cut-off values. The constructions' internal consistency and dependability are established by satisfying the two requirements, as suggested by the literature (Hair et al., 2017).

Discriminant validity

Verifying the constructs' discriminant validity is the third stage in the examination of the measurement model. The Fornell-Larker criterion, which states that all off-diagonal values should be smaller than the diagonal values, is examined. The correlations of each construct with itself must be higher than any values with other constructs to attain discriminant validity. The diagonal values which represent the square roots of the AVEs were bigger in all cases where the diagonal values in the following rows and columns are also diagonal values. As a result, when the Fornell-Larker criterion was examined, no apparent violations are found, and this research showed discriminant validity.

The structural model fit

The standardized mean square residual (SRMR), which compares the observed and indicated correlations in the model, is a suggested fit metric (Hair et al., 2017). The SRMR values obtained after running the analysis in the SmartPLS 4 program and executing the evaluation were in the suggested range. This means that the model obtained a satisfactory fit as the values of SRMR were in the range of 0.06 to 0.07, which is lower than the suggested threshold of 0.08. In this instance, the investigation confirmed the model's good match with the data and further strengthens the findings from earlier parts. As a result, the research's model is validated by its correctness, applicability, and strong match. The measurement model demonstrated its internal consistency reliability, convergent validity, and discriminant validity based on the analysis and results from the previous three steps. Therefore, it is acceptable and justified to evaluate the structural model in the next section. Figure 2 affords a summary of the measurement model assessment.

Hypothesis testing

Table 1: Path coefficients and hypothesis testing

Path (mean/SD)	Path coefficients	T-values	P-values	CI 2.5%	CI 97.5%	Decision
TOV -> CSF	-0.255	5.684	0.000**	-0.326	-0.151	Rejected
TIN -> CSF	0.221	5.070	0.000**	0.129	0.302	Accepted
TCO -> CSF	0.151	3.064	0.002**	0.064	0.254	Accepted
TIS -> CSF	0.196	3.449	0.001**	0.071	0.292	Accepted
TUC -> CSF	-0.184	5.357	0.000**	-0.267	-0.130	Rejected
CTA x TCO -> CSF	0.113	2.522	0.012**	0.022	0.194	Accepted
CSF ->CCI	0.055	1.103	0.270**	-0.045	0.151	Rejected

Note. **p<0.05

Moderation analysis

Analysis was performed to determine the moderating effect of cybersecurity training and awareness, and cybersecurity monitoring on the relationship among techno stressors and cybersecurity fatigue. The moderating effect of cybersecurity training and awareness on the path from TCO to CSF is shown to be

statistically significant, while it is not for all the other paths (i.e., from TOV to CSF, from TIN to CSF, from TIS to CSF, from TUC to CSF). In addition, cybersecurity monitoring demonstrated no significant moderating effect on all the paths.

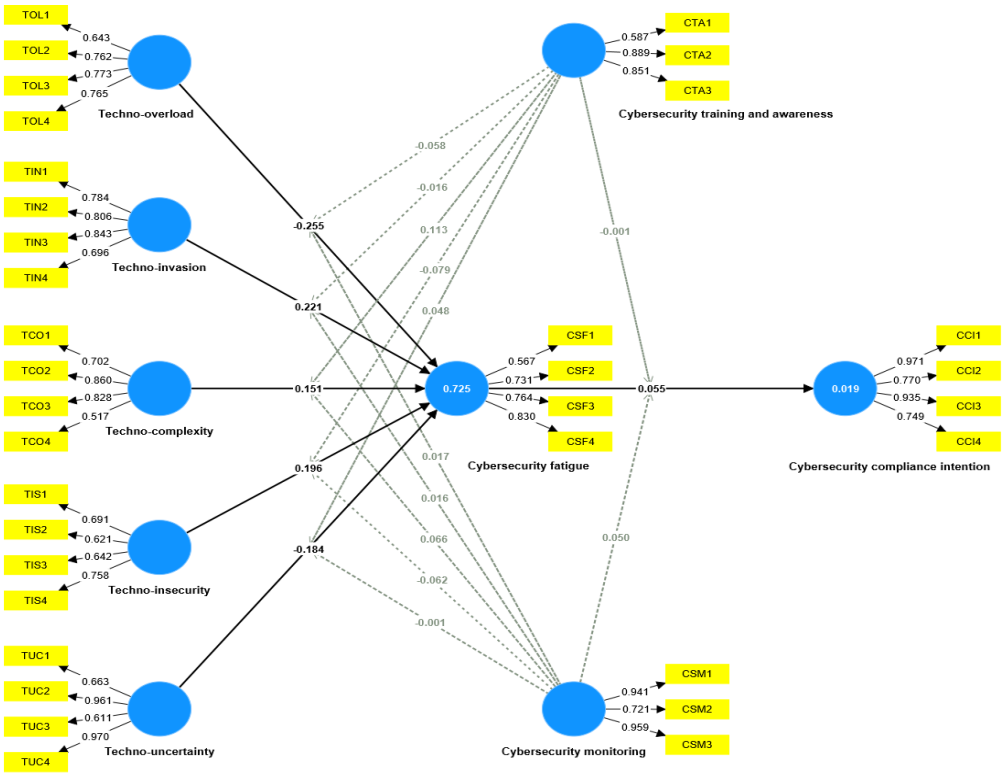

Figure 2: Measurement model assessment

Findings and discussion

The purpose of the current study is to comprehend the impact of technostress creators (techno-overload, techno-complexity, techno-insecurity, techno-invasion and techno-uncertainty) on the development of cybersecurity fatigue. This study proposes a structural model based on the technostress creators' model, including cybersecurity training and awareness, cybersecurity monitoring as possible moderators to cybersecurity fatigue. The impact of cybersecurity fatigue on compliance intention depending on the fatigue levels from the antecedents. The analysis generated eloquent findings to answer the research questions as discussed in the sections below. The proceeding sections answers the research questions by discussing the results of the study in relation to the hypotheses and literature.

Answering research question 1: *What is the impact of technostress creators on cybersecurity fatigue?*

Through hypotheses H1, H2, H3, H4 and H5, interestingly, results revealed a significant negative relationship between techno-overload and cybersecurity fatigue, rejecting H1. Ayyagari et al. (2011) denotes overload as the misfit between environmental demands and an individual's coping abilities. Overload has been identified as a core factor that leads to negative consequences from a behavioral and psychological perspective (Misra & Stokols, 2011; Karr-Wisniewski & Lu, 2010). Cook and Van Belle (2022), found that technostress negatively impacted university students' productivity and performance. For example, in the case of social media use, Lee et al. (2016) found that information overload, communication

overload and system failure affect social media fatigue. In addition, Molino et al. (2015) confirmed the negative impact of workload on behavioral stress. The negative relationship between techno-overload and cybersecurity fatigue in the current study may be explained by the fact that increased use of technology did not necessarily result in increased cybersecurity compliance information, communication and system failures that potentially lead to cybersecurity fatigue. Alternatively, university academics may have developed better coping mechanisms in environments of increased load and may not associate such technological overload with cybersecurity fatigue.

Furthermore, analysis revealed a significant positive relationship between techno-invasion and cybersecurity fatigue, confirming H2. The result is in line with Choi and Jung (2018), who reported that individuals can display signs consistent with burnout when they have an obligation to handle stressful workplace demands (i.e., overload). Choi and Jung (2018) further found that employees may disengage from online privacy issues and divulge private information, which the current study argues to be characteristics of cybersecurity fatigue. Techno-invasion is undoubtably a threat to mental and cognitive abilities of academics and is an element for consideration in promoting cybersecurity. In addition, results revealed a significant positive relationship between techno-complexity and cybersecurity fatigue, confirming H3. The result is consistent with the work by D'Arcy et al. (2014) who identified that techno-complexity is relevant to cybersecurity. Support is given by Hwang (2021), who found that technology driven techno-complexity had an impact on policy resistance being driven by anxiety and fatigue. Results further revealed a significant positive relationship between techno-insecurity and cybersecurity fatigue, confirming H4. The result may be an indicative of academics who become scared of losing their jobs to other people who have superior ICT knowledge. Older academics may be uncertain being driven by the fear of the younger generation (digital citizens), whom ICT knowledge is usually at superior level (Tarafdar et al., 2017).

Furthermore, analysis revealed a significant negative relationship between techno-uncertainty and cybersecurity fatigue, rejecting H5. Techno-uncertainty pertains to constant technological changes, which may be a source of stress for individuals. Interestingly, results suggest that stress from such constant technological changes does not lead to academics' cybersecurity fatigue. The finding contradicts previous findings which demonstrate that techno-uncertainty leads to undesirable consequences, for example by a study by Alam (2016), found that techno-uncertainty had undesirable consequences on productivity in the aviation industry. As purported by Tarafdar et al. (2011), techno-insecurity denotes stressful circumstances that make individuals feel "threatened about losing their jobs to other people who have a better understanding of technology", p.117. Therefore, the current study demonstrates that the anxiety from the possibility of losing jobs did not have a bearing on cybersecurity fatigue among university academics. Two techno-stressors demonstrated negative association with cybersecurity fatigue: techno-overload (H1) and techno-uncertainty (H5) This may be because the mechanisms fundamental to techno-overload and techno-uncertainty are deeply connected to an environment that is continuously changing and disrupted, as is in the case of higher education during the emergency remote teaching period.

Answering research question 2: *How does cybersecurity monitoring, training and awareness moderate the relationship between techno stressors and cybersecurity fatigue?*

Results demonstrated that cybersecurity training and awareness has significant positive moderating effect on the relationship between techno-complexity and cybersecurity fatigue (in other words training and awareness dampens the positive relationship between techno-complexity on cybersecurity fatigue). However, this contradicts with findings in literature (D'Arcy et al., 2014; Stanton et al., 2016), whose studies found that advice related to cybersecurity may result in employees feeling exhausted especially when they doubt the efficacy of the training and awareness interventions or security policies. Several

employees observe that the cybersecurity systems such training, awareness and monitoring mechanisms at their workplaces further complicate their lives (Calic et al., 2016; Stanton et al., 2016). Therefore, the current study observes that interventions aimed at addressing cybersecurity are necessary for university academics. However, in relation to Reeves et al. (2021) propositions, such interventions should ponder the probable additional stress this may exert on employees.

Answering research question 3: *How does cybersecurity fatigue relate to cybersecurity compliance intention?*

Results demonstrate that cybersecurity fatigue has an insignificant positive influence on academics' cybersecurity compliance intention. The results diverge with literature, for example Stanton et al. (2016) and Reeves et al. (2021) who separately demonstrated that cybersecurity fatigue leads to individuals becoming overwhelmed, tired and frustrated from work pressures and stresses thereby becoming careless in their day-to-day security related behaviors. The fatigued individuals no longer engage with cybersecurity protocols and advice (D'Arcy et al., 2014; Choi & Jung, 2018). Current study findings disagree with literature as academics are a different set of professionals leading them to behave differently.

Conclusion, Implications, Limitations, and Future Work

The main aim of the current study was to determine the effects of technostress creators on cybersecurity fatigue. The study makes several recommendations to reduce the stress that may be experienced by academics because of the adoption of IS security measures, policies and technology. By incorporating human-centred initiatives to avoid the degrading of human performance and learning from other industries, universities may strengthen cybersecurity processes. To lessen the likelihood of the universities being the victim of a successful cyber-attack or incident, stress, burnout, and security fatigue are human risk factors that need to be mitigated and eliminated. The study further recommends integrating elements of counselling and employee wellness programmes during technological innovations and integration. These initiatives, in turn, assist to reduce the perception of the complexity, insecurity, invasion, overload, and uncertainty an employee may experience when using technology for work. Cybersecurity promotion initiatives of training and awareness need to be advanced in moderation. The initiatives should not add extra burden to academics, leading to further fatigue. Despite the current study affording interesting results on cybersecurity in the higher education environment, the study is short of generalisability as sampling concentrated on academics from one institution of higher education. Future longitudinal studies may focus on a larger sociocultural diverse sample from various institutions of higher education in South Africa.

Ethical considerations

The study followed ethical considerations processes. The research approval was granted by the Durban University of Technology's Institutional Research Ethics Committee (IREC) under ethics clearance number: IREC 088/22, after assessment to ensure that participants' rights of anonymity, confidentiality, privacy, informed consent were observed.

References

Ahmad, U. N. U., Amin, S. M. & Ismail, W. K. W. (2012). The Relationship Between Technostress Creators and Organisational Commitment Among Academic Librarians. Procedia Social and Behavioral Sciences, 40, 182 - 186. https://doi.org/10.1016/j.sbspro.2012.03.179

Alam, M. A. (2016). Techno-stress and productivity: Survey evidence from the aviation industry. *Journal of Air Transport Management*, *50*, 62-70. https://doi.org/10.1016/j.jairtraman.2015.10.003

Andrade, C. (2019). Describing research design. *Indian journal of psychological medicine*, *41*(2), 201-202. https://doi.org/10.4103%2FIJPSYM.IJPSYM_66_19

Atanasoff, L., & Venable, M. A. (2017). Technostress: Implications for adults in the workforce. The Career Development Quarterly, 65(4), 326–338. https://doi.org/10.1002/cdq.12111

Ayyagari, R. (2008). What and why of technostress: Technology antecedents and implications. Dissertation Abstracts International Section A: Humanities and Social Sciences, 68(11-A), 4762.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS quarterly*, 831-858. https://doi.org/10.2307/41409963

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & security*, *39*, 145-159. https://doi.org/10.1016/j.cose.2013.05.006

Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education. Comput. Secur. 2019, 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Brehm, J. (1966). A theory of psychological reactance. Academic Press.

Brillhart, P.E. 2004. Technostress in the workplace: Managing stress in the electronic workplace. *Journal of American Academy of Business*, *5*(1/2), pp.302-307.

Brod, C. (1984). *Technostress: The human cost of the computer revolution*. Reading, Mass.: Addison-Wesley.

Buchtel, E. E., Guan, Y., Peng, Q., Su, Y., Sang, B., Chen, S. X., & Bond, M. H. (2015). Immorality east and west: Are immoral behaviors especially harmful, or especially uncivilized?. *Personality and Social Psychology Bulletin*, *41*(10), 1382-1394.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548. https://doi.org/10.2307/25750690

Calic, D., Pattinson, M., Parsons, K., Butavicius, M., & McCormac, A. (2016, July). Naïve and accidental behaviours that compromise information security: What the experts think [Paper presentation]. The Tenth International Symposium on Human Aspects of Information Security & Assurance.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188. https://doi.org/10.2753/mis0742-1222290305

Choi, H., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Clute, R. (1998). Technostress: A Content Analysis: Kent State University.

Cook, G., & Van Belle, J. P. (2022). Analysis of technostress experienced by students at the university of cape town, during the COVID-19 pandemic. *Issues in Information Systems*, *23*(1). https://doi.org/10.48009/1_iis_2022_106

D'Arcy, J., Herath, T., Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. Journal of Management Information Systems, 31(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98. http://www.jstor.org/stable/23015462

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43-69. https://doi.org/10.1111/isj.12173

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in human behavior*, *26*(6), 1739-1747. https://doi.org/10.1016/j.chb.2010.06.023

Department of Justice and Correctional Services. (2017). *Cybercrimes and Cybersecurity Bill.* Pretoria.
Donalds, C., & Osei-Bryson, K. M. (2017). Exploring the impacts of individual styles on security compliance behavior: A preliminary analysis. In *SIG ICT in Global Development, 10th Annual Pre-ICIS Workshop, Seoul, Korea*.
Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*, 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056
Fenner, G. H., & Renn, R. W. (2010). Technology-assisted supplemental work and work-to-family conflict: The role of instrumentality beliefs, organizational expectations and time management. *Human Relations*, *63*(1), 63-82. https://doi.org/10.1177/0018726709351064
FireEye, Inc. Cyber Threats to the Education Industry. White Paper, 2016. Library Catalog. Available online: www.fireeye.com (accessed on 10 March 2022).
Furnell, S., Thomson, K.-L. (2009). Recognising and addressing "security fatigue." Computer Fraud & Security, 2009(11), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3
Garrison, C. Lessons learned from university data breaches. Palmetto Bus. Econ. Rev. 2010, 13, 27–37. 3.
Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: an update and extension to SEM guidelines for administrative and social science research. *MIS quarterly*, iii-xiv. https://doi.org/10.2307/23044042
Grant, C. A., Wallace, L. M., & Spurgeon, P. C. (2013). An exploration of the psychological factors affecting remote e-worker's job effectiveness, well-being and work-life balance. *Employee Relations*. https://doi.org/10.1108/er-08-2012-0059
Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Partial least squares structural equation modeling (PLS-SEM) using R: A workbook. https://doi.org/10.1007/978-3-030-80519-7
Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). *Advanced issues in partial least squares structural equation modeling*. saGe publications.
Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). SAGE Publications, Inc.
Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. (2017). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial management & data systems*. https://doi.org/10.1108/imds-04-2016-0130
Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52-65. https://doi.org/10.1016/j.cose.2016.12.016
Henson, R., Stewart, G., & Bedford, L. (2020). Key challenges and some guidance on using strong quantitative methodology in education research. *Journal of Urban Mathematics Education*, *13*(2), 42-59. https://doi.org/10.21423/jume-v13i2a382
Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005
Hickman, R. L., Pignatiello, G. A., & Tahir, S. (2018). Evaluation of the decisional fatigue scale among surrogate decision makers of the critically ill. Western Journal of Nursing Research, 40(2), 191–208. https://doi.org/10.1177/0193945917723828
Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5). sage.
Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information systems research*, *25*(1), 111-136. https://doi.org/10.1287/isre.2013.0501
Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security

policy abuse by employees?. *Communications of the ACM*, *54*(6), 54-60. https://doi.org/10.1145/1953122.1953142

Hwang, I. H. (2021). The influence on the information security techno-stress on security policy resistance through strain: Focusing on the moderation of task technology fit. *The Journal of the Korea institute of electronic communication sciences*, *16*(5), 931-940.

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*. https://doi.org/10.1108/oir-11-2015-0358

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79. https://doi.org/10.1016/j.im.2013.10.001

Insiders, C. (2018). Insider threat-2018 report. *CA Technologies. Accessed Jun*, *20*. Retrieved from https://crowdresearchpartners.com/portfolio/insider-threat-report/

Karr-Wisniewski, P., & Lu, Y. (2010). When more is too much: Operationalizing technology overload and exploring its impact on knowledge worker productivity. *Computers in Human Behavior*, *26*(5), 1061-1072. https://doi.org/10.1016/j.chb.2010.03.008

Latan, H., Ringle, C. M., & Jabbour, C. J. C. (2018). Whistleblowing intentions among public accountants in In_donesia: Testing for the moderation effects. Journal of Business Ethics, 152(2), 573-588. https://doi.org/10.1007/s10551-016-3318-0

Lee, A. R., Son, S.-M., & Kim, K.K. (2016). Information and communication technology overload and social networking fatigue: A stress perspective. Computers in Human Behavior 55, 51-66. https://doi.org/10.1016/j.chb.2015.08.011

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

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Information Systems Journal, 25(5), 433–463. https://doi.org/10.1111/isj.12043

Lu, Y., & Da Xu, L. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115. https://doi.org/10.1109/jiot.2018.2869847

Maier, C., Laumer, S., Weinert, C., & Weitzel, T. (2015). The effects of technostress and switching stress on discontinued use of social networking services: a study of Facebook use. *Information Systems Journal*, *25*(3), 275-308. https://doi.org/10.1111/isj.12068

Misra, S., & Stokols, D. (2011). Psychological and health outcomes of perceived information overload. Environment and Behavior. https://doi.org/10.1177/0013916511404408

Molino, M., Cortese, C. G., Bakker, A. B., & Ghislieri, C. (2015). Do recovery experiences moderate the relationship between workload and work-family conflict?. *Career Development International*. https://doi.org/10.1108/cdi-01-2015-0011

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS quarterly*, *42*(1). https://doi.org/10.25300/misq/2018/13853

Ng, B. Y., & Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. *PACIS 2007 Proceedings*, 45.

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. https://doi.org/10.1016/j.dss.2008.11.010

Norton South Africa (2012) *Norton cybercrime report 2012.* Retrieved from http://za.norton.com/cybercrimereport/promo?inid=uk hho downloads home link cybercrimereport

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156b-156b). IEEE. https://doi.org/10.1109/hicss.2007.206

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. Security and Privacy Protection in Information Processing Systems–IFIP Advances in Information and Communication Technology, 405, 366–378. https://doi.org/10.1007/978-3-642-39218-4_27

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016b, July). The information security awareness of bank employees. In N. Clarke & S. Furnell (Eds.), International Conference on Human Aspects of Information Security & Assurance.

Posey, C., Bennett, B., Roberts, T., & Lowry, P. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. https://www.semanticscholar.org/paper/When-Computer-MonitoringBackfires%3A-Invasion-of-and-Posey-Bennett/68f885ee5766 a88717f7246c878fe8b63c0c9e91

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management*, *51*(5), 551-567. https://doi.org/10.1016/j.im.2014.03.009

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778. https://doi.org/10.2307/25750704

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information systems research*, *19*(4), 417-433. https://doi.org/10.1287/isre.1070.0165

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open*, *11*(1), https://doi.org/10.1177/21582440211000049

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's comments: a critical look at the use of PLS-SEM in" MIS Quarterly". *MIS quarterly*, iii-xiv. https://doi.org/10.2307/41410402

Ringle, C. M., Wende, S., & Becker, J. M. (2015). SmartPLS 3 [software]. *Bönningstedt, Germany: SmartPLS*.

RSA. (2002b). Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) 70 of 2002.

RSA. (2009). Protection of Personal Information (POPI) Bill 9 of 2009.

RSA. (2013). Protection of Personal Information (POPI) Act 4 of 2013.

SABC News. (2017, April 19). Cyber-attacks reaching a critical point in SA. Retrieved from http://www.timenews.co.za/timenews-sabc-news-cyber-attacks-reaching-a-critical-point-in-sawednesday-19-april-2017

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Salanova, M., Llorens, S., & Ventura, M. (2014). Technostress: The dark side of technologies. In *The impact of ICT on quality of working life* (pp. 87-103). Springer, Dordrecht. https://doi.org/10.1007/978-94-017-8854-0_6

Salo, M., Pirkkalainen, H., & Koskelainen, T. (2019). Technostress and social networking services: Explaining users' concentration, sleep, identity, and social relation problems. *Information Systems Journal*, *29*(2), 408-435. https://doi.org/10.1111/isj.12213

Sang, Y., Lee, J.-K., Kim, Y., & Woo, H.-J. (2015). Understanding the intentions behind illegal downloading: A comparative study of American and Korean college students. Telematics and Informatics, 32(2), 333-343. https://doi.org/10.1016/j.tele.2014.09.007

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

Song, S. (2017). African undersea cables - Interactive. Many Possibilities blog. Retrieved from https://manypossibilities.net/african-undersea-cables-interactive

Srivastava, S. C., Chandra, S., & Shirish, A. (2015). Technostress creators and job outcomes: theorising the moderating influence of personality traits. *Information Systems Journal*, *25*(4), 355-401. https://doi.org/10.1111/isj.12067

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. IT Professional, 18(5), 26–32. https://doi.org/10.1109/mitp.2016.84

Stanton, J. M., & Stam, K. R. (2008). *The visible employee: using workplace monitoring and surveillance to protect information assets--without compromising employee privacy or trust*. Information Today, Inc. https://doi.org/10.1108/00242530810911923

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, *24*(2), 124-133. https://doi.org/10.1016/j.cose.2004.07.001

State Security Agency (SSA). (2015). *National cybersecurity policy framework.* Pretoria.

Suhag, A., & Daniel, A. (2023). Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense. *Journal of Cyber Security Technology*, *7*(1), 21-51. https://doi.org/10.1080/23742917.2022.2135856

Tarafdar, M., Cooper, C. L., & Stich, J. F. (2017). The technostress trifecta-techno eustress, techno distress and design: Theoretical directions and an agenda for research. *Information Systems Journal*, *29*(1), 6-42. https://doi.org/10.1111/isj.12169

Tarafdar, M., Pullins, E. B., & Ragu-Nathan, T. S. (2015). Technostress: negative effect on performance and possible mitigations. *Information Systems Journal*, *25*(2), 103-132. https://doi.org/10.1111/isj.12042

Tarafdar, M., Tu, Q., & Ragu-Nathan, T. (2010). Impact of technostress on end-user satisfaction and performance. Journal of Management Information Systems, 27(3), 303–334. https://doi.org/10.2753/mis0742-1222270311

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The impact of technostress on role stress and productivity. *Journal of management information systems*, *24*(1), 301-328. https://doi.org/10.2753/mis0742-1222240109

Tarafdar, M., Tu, Q., Ragu-Nathan, T. S., & Ragu-Nathan, B. S. (2011). Crossing to the dark side: examining creators, outcomes, and inhibitors of technostress. *Communications of the ACM*, *54*(9), 113-120.

Telstra Corporation. (2018). Telstra Security Report 2018. https://insight.telstra.com.au/content/dam/insight/pdfs/Telstra_Security_Report_2018_PDF_FINAL.PDF

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Wang, L., & Jones, R. (2020). Data analytics for network intrusion detection. *Journal of Cyber Security Technology*, *4*(2), 106-123. https://doi.org/10.1080/23742917.2019.1703525

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105. https://doi.org/10.1057/ejis.2009.12

Zhang, S., Zhao, L., Lu, Y., & Yang, J. (2016). Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social networking services. Information & Management 53, 904-914. https://doi.org/10.1016/j.im.2016.03.006