Understanding SME employees' security behaviours when performing work tasks using BYOD from multiple work locations

By:

Aigbefo Queen A.

45020442

Supervisors

Dr Yvette Blount and Dr Mauricio Marrone

A thesis submitted to Macquarie University

Department of Accounting and Corporate Governance

For the degree of Master of Research

June 2018

Table of Contents

Abstract

The focus of this study is to examine the security behaviours of SME employees who unintentionally misuse information systems or do not comply with security policies when working from multiple locations using BYOD. SMEs underestimate the security risk their employees may encounter when working from locations other than a central office location. SMEs have resource constraints (human and financial capital) that preclude them from focusing on protecting information assets. At the same time, SMEs attract talent by offering flexible work arrangements such as working from home, a co-working centre or other locations other than the office (anywhere working).

This study investigated factors that explain SME employees' security behaviour. The constructs for the theoretical model were developed from protection motivation theory, the theory of planned behaviour, habit, hardiness and stress. The constructs were empirically validated using data collected from 294 SME employees. The results of the study show that hardiness, stress and habit have a significant impact on employee's security intentions when working from multiple locations using BYOD. The study contributes to information security study by highlighting the importance of an employee's hardiness personality trait in framing their positive security behaviour.

Statement of Originality

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Date: 19/06/2018

Aigbefo Queen A.

To my mum

Acknowledgements

I thank God for the opportunity to be part of the Macquarie University research community. I could not have orchestrated the perfect timing of my whole experience.

I would like to acknowledge the contributions of people who have helped me in the research process. First, I am grateful to God for my supervisors and would like to express my heartfelt gratitude and thanks to, Dr Yvette Blount and Dr Mauricio Marrone for their advice, support, guidance and suggestions throughout the research process. I could not have imagined a better team to mentor and shaped me into the researcher I am turning out to be. Thank you.

I am also thankful for every resource person in the department of Accounting and Corporate Governance, who provided me with assistance in this research journey, especially Dr Ilja Nastjuk and Dr Frank Song.

Finally, I would like to thank my family, loved ones, friends and other research colleagues for their encouragements and supports. Thank you.

List of Tables

List of Figures

Chapter 1: Introduction

Information and communications technology (ICT) has transformed the way individuals live, how organisations carry out business and how the government interacts with citizens. Individuals can access vast amounts of resources, businesses and exchange personal information and services irrespective of their location using broadband internet and high-performance personal devices such as mobile phones, laptops and tablets. Personal data and business sensitive information are vital assets constantly targeted in security breaches (Verizon, 2018). The media reports on data breaches involving high profile organisations on an almost daily basis. For example, in May 2017, a massive ransomware crypto worm called WannaCry attacked over 300,000 computers in more than 150 countries, encrypting files, locking the systems and demanding users to pay a ransom between $300 and $600 for decryption of their files (EY, 2017).

There are 30 million small and medium-sized enterprises/businesses (SMEs) in the United States (US), over 2 million in Australia and 5.7 million in the United Kingdom. Large organisations often integrate their information technology (IT) resources, for example, their supply chain, with SMEs to enable seamless, real-time and up-to-date sharing of information to improve business operations (Huong Tran et al., 2016). Also, hackers target SMEs, seen as the weakest link, to access otherwise well-protected organisational security networks (Symantec, 2018).

Organisations have increased their spending on strengthening their IT security to combat information security risks and protect information assets from unauthorised access (SANS, 2016a). Information security operations are becoming more complex and sophisticated to match the changing tactics of attackers. However, SMEs are usually constrained financially and invest little in security which makes them easy prey to cyberattacks (Cisco, 2017). The incompatibility and sophistication of interconnected information systems between large organisations and partners that are often SMEs, provide an opportunity for hackers to exploit (Huong Tran et al., 2016).

1.1 Background

Since the beginning of the new millennium, technology and access to the internet have changed how organisations collect, store, and protect information. Therefore, organisations need security measures to protect their information systems along with the changes in communication, information storage and retrieval technologies (Dhillon and Backhouse, 2000).

Interconnectedness and networking of IT systems over the internet have enabled access to organisational information assets from any location (such as home, cafes, library amongst others). Boards and executive management realised that protection of information assets is vital to the business because data breaches involve serious consequences (von Solms and von Solms, 2005). Organisations that experience a data breach may have to pay excessive fines to regulatory bodies, pay customers whose records were compromised and deal with damage to brand name or reputation (Layton and Watters, 2014). Spanos and Angelis (2016) found that information security events such as data breaches have a significant effect on the stock price of affected organisations. A recent survey of business that suffered from data breaches in 2017 found that 60 per cent of SMEs go out of business within six months of an attack (UPS Capital, 2017).

The humans within an information security system can be both a threat (a potential cause of an unwanted incident) and a vulnerability (a weakness that can be exploited) when accessing information assets (Furnell and Clarke, 2012). In September 2017, Deloitte, one of the world's largest accountancy and consultancy firm was the target of a data breach (The Guardian, 2017). An administrator's account which was not properly secured gave the attackers privileged and unrestricted access to Deloitte's confidential data and some of its clients (Deloitte, 2017). After the attack, Deloitte's management implemented an overall security architecture to improve employee's security privileged access. The case of Deloitte shows that employees need to understand that security threats may arise from their work actions and thus develop security behaviours to minimise external unauthorised access to organisational information assets (Rocha Flores and Ekstedt, 2016).

Employees may violate security policies when working, for example, copying sensitive information to their personal devices due to constant mobility or to improve their job performance (Guo et al., 2011). D'Arcy and Devaraj (2012) suggested that employees who spend more hours of work away from the office are more inclined to not adhere to organisational policies. Therefore, more studies are needed to understand employees' security behaviours and the factors that may promote secured behavioural practices.

Employees are the weakest link in information security system (Yildirim et al., 2011) which has prompted researchers to investigate employees' security behaviour. However, there are few studies focusing on how the use of BYOD influences employees' security behaviours. Similarly, previous studies have demonstrated that factors which influence employees' security behaviours have different effects depending on the security context. For example, some employees' security behaviours may be influenced by fear within the organisation (Johnston and Warkentin, 2010), while other employees' behaviours are subject to affective influence (state of emotional feeling) (D'Arcy and Lowry, 2017). Although factors identified in previous research have improved our understanding of employees' security behaviour, there is still a need to investigate security behaviours in a different context because technology and work trends within organisations are evolving (Crossler et al., 2013). The next section outlines the research question and aim of the study.

1.2 Research Aim and Question

An information breach may or may not have direct consequences for employees. Also, security knowledge may not always be generalised across all work context (Thompson et al., 2017). To better understand employee security behaviours in different work contexts, the main research aim is to investigate the security behaviour of SME employees when using personal devices (BYOD) for work purposes from multiple work locations. Specifically, this study will examine the following research question:

How do the type of work tasks and locations of work change SME employee security behaviour when using personal devices?

1.3 Motivation for the study

As outlined above, we need a better understanding of factors that may influence employee security behaviours in small and medium-sized organisations. An understanding of these factors will provide insights to researchers and SMEs on how to create security policies and procedures to guide an employees' perception of security behaviours when working from alternative work locations.

There is a growing concern for the information security of SMEs because they are essential to business supply chains and play a vital role in growing a nation's economy. In 2017, 61% of security breaches were in SMEs when compared to the previous year's 53% (Verizon, 2018). SMEs usually underestimate their level of security exposure to threats. SMEs assume that hackers are more interested in large organisations, and with regards to their size, security risk mitigation will be easier (Ng et al., 2013). Therefore, SMEs employees require more security awareness to enable them to protect organisational information assets.

Employees accessing organisational information assets such as work emails and sensitive business information with their personal device may create security vulnerabilities for the organisation. Organisations, especially SMEs, claim that BYOD and smart devices are considered high security risks to information security management (Cisco, 2017). Employees working from multiple locations may inadvertently perform actions such as connecting to a public Wi-Fi and access sensitive information, and potentially expose organisational information assets to security threats (Agudelo et al., 2015). Crossler et al. (2014) discovered that SME employees are often not aware of their organisation's BYOD policy requirements which could lead to potential information security breaches.

Despite security policies within organisations, employees are the major sources of data breaches. Scholars have carried out numerous studies to understand why employees behave in an unsecured manner despite being aware of security policies (Johnston and Warkentin, 2010; Puhakainen and Siponen, 2010). Puhakainen and Siponen (2010) found that some employees' security training are not effective because the approaches are largely unscientific and atheoretical resulting in less systematic cognitive processing of the training information. This study will provide insights for researchers and SMEs on factors that influence employee's perceptions of security behaviour when using their personal device working in different locations.

The study will inform practitioners on how security risks may be mitigated to lower potential security vulnerabilities targeted towards their information assets from an employee's actions. In 2018, the average cost of a data breach reported rose from $U3.62 in 2017 to $U3.86 million and third parties breaches also further increases the cost of a breach (Ponemon, 2018). Organisations partnering with SMEs as part of their supply chain network require knowledge of factors that will positively influence SME employee's security behaviour when connecting or accessing their information assets from multiple geographical locations using personal devices.

1.4 Thesis outline

The remaining chapters of the thesis are organised as follows: Chapter 2 provides a review of the relevant literature relating to behavioural information security. The literature review synthesises the literature on technology and work trends that may create security risks for SMEs, common information security standards and frameworks used to create information security policies and previous studies on information security behaviour.

The theories used to frame the research are presented in Chapter 3. Based on the literature explored in chapter 2, the theoretical model for the study is explained.

Chapter 4 explains the research design and methodology used to answer the research question. The justification for using a quantitative data collection and analysis procedure is discussed.

Chapter 5 provides the data analysis. A psychometric test is conducted on the data to assess the reliability and validity. The results of the data are presented.

Chapter 6 is the discussion of the results and findings from the study. The theoretical and practical contributions of the study are discussed.

Finally, in chapter 7, the conclusions of the research are outlined, along with the research limitations and areas for future research is identified.

Chapter 2: Review of literature

2.1 Introduction

This chapter presents the literature used to frame and gain an understanding of the research aim. The chapter begins by exploring technology trends, changes in the workplace (work location and task), and the security risks they create. Then an overview of information security standards and frameworks that organisations use to create their information security policies (ISP). The final section examines the literature on employee information security behaviours and the SME security context.

Organisations, governments and private individuals are increasingly concerned about the security of sensitive and personal information (such as financial and health data) being shared, exchanged and stored (Chen et al., 2012). Technology trends including the Internet of Things (IoT), Cloud computing, artificial intelligence and machine learning, and work trends such as bring your own device (BYOD), employee work arrangements such as freelancers, part-time workers, and consultants contribute to the increased risk of data breaches. Organisations adopt new technologies and work trends to encourage employees to innovate, maintain good work-life balance, or boost their reputation to attract future employees (Graber, 2015; Weeger et al., 2016). Furthermore, the employees in small and medium-sized enterprises/businesses (SMEs) are the most targeted for cyber-attacks in 2017 when compared with previous years (Symantec, 2017).

2.2 Technology and Work trends

This section evaluates technology trends that SMEs have adopted as well as work trends that have been enabled by new technologies.

2.2.1 Technology trends: Bring Your Own Device, Internet of Things, Cloud Computing, and Real-time Collaboration

The continual decrease in prices of personal and mobile computing has made it possible for individuals to purchase information and communication technology (ICT) devices such as laptops, smart phones, and tablets, for both personal and work use. The use of personal computing devices in the workplace gave rise to the trend of Bring Your Own Device (Olalere et al., 2015). The Bring Your Own Device (BYOD) or Bring Your Own Technology (BYOT) allows employees to use their preferred personal devices for work. BYOD is often preferred by the user because they are more likely to be the latest technology and employees are more familiar with the device (Blount, 2017). Employees believe they are more efficient and productive using their own device for work task (Olalere et al., 2015; Vandelannoitte, 2015). The benefits of BYOD for the organisation include employee retention, work flexibility, employee connectivity enabling them to work at anytime and anywhere, and reduced operational cost (Pyöriä, 2011; Sebescen and Vitak, 2017).

Ubiquitous broadband internet and wireless technology networks available in public locations have enabled more mobile users to stay connected via their devices. Connectivity is enabled by not just laptops and mobile phones but also smart devices, wearables (embedded smart devices worn on the human body such as Fitbit), data, social networks, and multimedia content, all of which culminates in the Internet of Things (IoT) (Holtgrewe, 2014). Organisations interconnect with each other to enable seamless communication between technology systems, integrate with partners, vendors and other stakeholders, business analytics systems and intelligent applications. However, IoT is expected to multiply information security threats due to the increased interconnectivity of personal devices to the internet (Sicari et al., 2015).

Cloud computing facilitates IoT by offering unlimited storage and processing power, providing scalability, interoperability, flexibility, reliability, efficiency, and availability (Botta et al., 2016). The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (NIST, 2011). Cloud computing offers organisations a distributed system of computer resources over the internet (Sadiku et al., 2014), enabling employees to access organisational networks, applications and information assets from anywhere at any time. Over ubiquitous internet and technology infrastructure, cloud computing has facilitated SMEs agility and scalability, fostering global collaboration between individuals and organisations (Botta et al., 2016). Cloud service providers offer different levels of technology service tools to clients for easy accessibility such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) amongst others (Sadiku et al., 2014). For example, Microsoft Azure is offered as a PaaS enabling an organisation and its employees to collaborate in real-time with other organisations and to exchange data and services.

The literature on cloud computing shows that top management support, firm size and business environment amongst other factors play an important role in the adoption of cloud technologies in organisations (Alshamaila et al., 2013; Low et al., 2011). However, SMEs are increasingly adopting cloud platforms due to flexibility, relative advantage, and the cost savings cloud computing affords (Al-Isma'ili et al., 2016). BYOD, Cloud Computing, and IoT have facilitated anywhere working by enabling SMEs to better collaborate with partners, customers and stakeholders anytime, anywhere to achieve organisational objectives.

2.2.2 Work trends

The 19th and 20th centuries were characterised by mechanised labour and mass production of goods and services (largely manufacturing and factory jobs), where individuals commuted to central locations for work (Blount, 2015a). Communications and collaborative technologies such as emails, social media, cloud storage (Blount, 2017) as well as new ways of working such as knowledge work (more intuitive) and process work (more routine and repetitive) have changed the way work is designed and how employees work (Greene and Myerson, 2011). New technologies and types of work have facilitated employees working from other physical locations outside the traditional office building, for example, a home office, satellite centres or public places (Wojcak et al., 2016). Employees may have different work arrangements such as full-time, part-time work, freelancers, gig workers, contractors and consultants (Blount, 2015b; Healy et al., 2017). ICT advancement (Blount, 2015a), high cost of real estate and office running cost (Pyöriä, 2011), and government policies in some countries (such as the USA Telework Enhancement Act of 2010; Australia's Fair work Act 2009) have made it possible to work in different locations and redesign work tasks.

Scholars have used different terms to describe flexible work trends such as anywhere working, telecommuting, telework, working at home, work from home, or remote work among others (Blount, 2015a). For this study, the term anywhere working is used and refers to employees conducting their regular work activities from locations other than the regular office location (Vilhelmson and Thulin, 2016).

Ubiquitous internet and mobile technologies have enabled employees to access organisational information assets effectively and efficiently from multiple locations such as an airport lounge, cafes, restaurants, and even while commuting on high-speed rail (Blount, 2015a). Some organisations adopt anywhere working arrangements encouraging their employees to work from multiple locations such as hot-desks, co-working centres and non-territorial workspaces using BYOD devices. These alternative workspaces offer resources on demand, providing employees with a more traditional office atmosphere and the freedom of flexible hours to work (Johns and

Gratton, 2013). However, there is an on-going discussion among scholars and practitioners alike about the benefits and detriments of anywhere working.

2.2.3 Anywhere working: an on-going debate

The literature on anywhere working examines benefits and limitations for employees, organisations and society. Pyöriä (2011) reported benefits of anywhere work including the environmental friendliness, less traffic congestion, reduced environmental pollution as well as the safety of commuters resulting from lower risks of traffic accidents. Employees with anywhere working arrangements also self-reported a higher level of productivity (Butler et al., 2007), increased work-life balance, greater job satisfaction and performance (Bentley, 2013; Morganson et al., 2010). Henke et al. (2016) reported reduced health risks for anywhere working employees. Martin and MacDonnell (2012) similarly reported improved productivity, retention, commitment and performance in the organisation when employees take up anywhere working.

On the other hand, some organisations have recently asked their employees to return to the office from working from home arrangements. Notably among these organisations are Yahoo (Humphry, 2013) and IBM (Weller, 2017), ordering all staff who have been allowed to work from home and those who work remotely back to the office. Both organisations cited the need for in-person collaboration as reasons for ordering staff back to the central office. Researchers have likewise recorded negative outcomes associated with anywhere working; most cited reasons are professional and social isolation (Allen et al., 2015; D'Arcy and Hovav, 2009). Professional isolation potentially excludes an employee from the workplace community due to their physical absence, which may threaten their career advancement (Pyöriä, 2011). While social isolation alters employees' relationship towards the organisation and reduces their engagement with the organisation (Golden, 2009). An employee's isolation may exclude them from organisational activities that allow them learn the organisational culture. Employees who imbibe the culture of the organisation are found to be more compliant with security policies (Hu et al., 2012). Bentley et al. (2016) found that individuals who work from anywhere experienced an increase in their psychological strain due to the absence of organisational social support.

These studies suggest that organisations need to assess the impact of anywhere working on employees' overall performance because some work roles within the organisation may not be suited for anywhere working. Kotey (2017) reported that some work roles in organisations such as agriculture, wholesale, retail and personal service sectors where physical presence is essential might not be suitable for working in alternative locations.

2.2.4 Autonomous work tasks

Taylor's Scientific Management Principles introduced the division of labour where tasks are broken down into smaller chunks and supervised by employees who are more knowledgeable (Taylor, 1911). Decades later work tasks are divided similarly to Taylor's principles, either as processed work where output can be easily measured and monitored (such as call centre agents) or knowledge-based work (Greene and Myerson, 2011). Knowledge-based work refers to work-related tasks that are highly autonomous, non-repetitive, requires skills and knowledge to organise and execute (Drucker, 1999). The level of autonomy for carrying out work tasks is an important criterion for assessing the suitability of anywhere working (Blount, 2015a). Work autonomy refers to the extent to which an employee has independence over work-related tasks (Allen et al., 2015).

Work tasks that are well-defined and where productivity is easily measured may be suitable for anywhere working. For example, data or language translators, data entry or call centre agents follow routines or perform repetitive tasks and can work from anywhere (Blount, 2015a). Blount (2017) advised that work which required accessing confidential and sensitive information may not be suited for anywhere work. Knowledge or process workers who access private data such as medical or financial records could work from certain secured locations, but it may not be appropriate for public places or co-working centres. SMEs are faced with the dilemma of protecting information assets from unauthorised access when employees sign up to work from multiple locations using BYOD (Bayrak, 2012).

2.3 Cybersecurity threat landscape

The growing dependence and adoption of information technology solutions and computer networks by individuals, governments and organisations have made information a valuable asset and an attractive target for cyber-attacks. Research has shown that cyber threats and attacks increase with emerging technologies (such as social media, cloud computing, mobile computing), and societies become largely dependent on computer networks and information technology daily (Jang-Jaccard and Nepal, 2014; Telstra, 2018).

Organisations usually rely on sophisticated technological solutions (software and hardware) to protect and secure access to information assets (Singh et al., 2013). However, hackers exploit vulnerabilities and weaknesses within the security systems to gain easy access to an organisation’s network, bypassing the sophisticated security solutions in place (Jang-Jaccard and Nepal, 2014).

Studies have identified humans (employees, third-party access) as the weakest link in the information security chain (Yildirim et al., 2011; PWC, 2018). Therefore, hackers employ social engineering attacks to exploit human weaknesses within the organisation’s information security systems. Social engineering refers to ploys used to influence people to divulge sensitive information or gain access to information assets (Mouton et al., 2016). Social engineering has become a major security threat to organisations often launched by hackers through social media, emails (phishing), phone (phone fraud) or physically by the theft of personal mobile devices (Jang-Jaccard and Nepal, 2014; Rocha Flores and Ekstedt, 2016). This has prompted information security researchers to examine factors that influence or determine the security behaviours of technology users (employees and end-user) (Crossler et al., 2013; Posey et al., 2015).

Organisations expose their employees to new security risks when they adopt new technologies and work trends. Creation of appropriate policies, training and increasing awareness can help ensure employees protect organisational information assets. It is now common for employees to use personal devices (BYOD) at work, wearables (such as Fitbits), or smartwatches that link to work emails (Martin, 2017). New ways of working (such as anywhere work) and new technologies may attract employees (Weeger et al., 2016) but may create security risks that become a point of vulnerability when mismanaged by employees. Management needs to assess security-related risks to enable them to select appropriate information security standards and frameworks to create security policies and properly mitigate against potential attacks on information assets. Several international security standards and frameworks are available to organisations and some specially designed for SMEs to guide them when creating security policies.

2.4 Information security frameworks and security policies

Research has shown that effective security of information assets within the organisation is everyone’s responsibility (Ifinedo, 2014; Safa et al., 2016). However, the board of directors and managers are accountable to the business when an information security breach occurs (Whitman and Mattord, 2012). Serious legal consequences and penalties could be levied on an organisation due to a data breach. For example, in 2017 a civil lawsuit was filed in the U.S. against Equifax, a credit reference agency, requesting it to pay $439 million for more than 145 million customers records that were compromised (McCrank and Finkle, 2018). Similarly, in the UK, the government issued TalkTalk fines totalling £500,000 for exposing personal information of more than 150,000 customers in the 2015 (Ashford, 2017). In Australia, Telstra, a telecommunications organisation, paid an infringement notice of $10,200 for contravening the Australian Communications and Media Authority (ACMA) directive in relation to a data breach which exposed more than 15,000 customer records (OAIC, 2014).

In Australia, the Notifiable Data Breaches (NDB) is an amendment to the Privacy Act 1988, making it mandatory for business owners to notify the relevant authorities and affected individuals whose personal information is compromised in a data breach (Privacy Amendment Act, 2017). Similarly, organisations handling personal information of European citizens will have to comply with the General Data Protection Regulation (GDPR) (EUGDPR, 2018) irrespective of their geographical location. While in the U.S, protecting personally identifiable information (PII) of individuals (such as name, email address, driver's license) is sectoral and regulated based on the category of the information, but data breaches are reported under the various US data-breach laws in each state (NCSL, 2018). SMEs collaborating or handling personal information (such as email addresses, bank details, medical information, or a computer IP address) have to be compliant with these data protection regulations or risk getting fines and reputational damage if data breaches occur.

Organisations create information security policies (ISP) from international standards, frameworks and regulations to guide the adoption of technology, work trend, and employee use and access to information assets. In the U.S, the government enacted the Cybersecurity Enhancement Act of 2014 (CEA) enabling the National Institute of Standards and Technology (NIST) to facilitate and support the development of a cybersecurity risk framework. The NIST framework provides a guide for organisations to assess risks, in considering the business drivers and security considerations specific to its use of technology (NIST, 2018). Information security frameworks and standards provide a generic methodology and model to follow in the setup, protection, and management of organisational information assets and critical infrastructure (ISO, 2016). Organisations, especially SMEs, adopting information security standards/frameworks have to consider the business objectives and IT strategies when creating security policies (Antonucci, 2017).

2.4.1 Information security standards and frameworks: Strengths and Weaknesses

There are many security standards and frameworks available to organisations to develop their ISP (see Table 1). Studies have compared some standards/frameworks to outline their strengths and weaknesses to provide a guide for organisations to formulate information security policies

(Susanto et al., 2011; Cram et al., 2017). However, adopting security standards and frameworks does not guarantee the effectiveness of an ISP to protect the organisation against a security breach (Flowerday and Tuyikeze, 2016). For example, the ISO 27000 series outline general requirements for establishing, implementing, maintaining and improving information security management systems, but organisations have to tailor these requirements to fit their security risks (Antonucci, 2017).

Table 1: Commonly used international security standards and frameworks (Antonucci, 2017) updated as of May 2018

Standard/ framework	**Issuer**	**Latest update**	**Type**	**Strength**	**Weakness**
ISO/IEC 27000	International Organisation for Standard (ISO)	2016	Information security, Risk, IT functions	Widely recognised and accepted, focused on threat mitigation	Specific to information security, limited scope and recommendations
COBIT 5 (Control Objectives for Information and Related Technologies)	ISACA	2012	All IT function, Information security, Risk	Globally accepted, allows part implementation, regular update based on recent technology	Leads to gap if not fully implemented, process-based, high level approach
NIST Cybersecurity framework	National Institute of Standards and Technology (NIST)	2018	All IT function, Information security, Risk	Risk based, easily implemented	Limited in scope to information security, gaps in implementation
Standard of Good practice for Information Security	Information Security Forum (ISF)	2016	All IT function, Information security, Risk	Addresses information security from a business perspective, detailed recommendations	Complex implementation due to broad security coverage
SANS top 20	The SANS Institute	2018	All IT function, Information security, Risk	List of top 20 widely adopted security controls, security recommendations	No metric for measuring success, high-level document
IT-CMF:ISM (IT Capability Maturity Framework-Information Security Management)	Innovation Value Institute	2016	IT management, Information security	Security maturity assessment, integration of other standards and frameworks	Focuses on large organisations,
PCI-DSS (Payment Card Industry Data Security Standard)	Payment Card Industry (PCI) Security Standards Council	2016	IT function, Information security	Compulsory to implement all control areas	Not flexible, restricted to credit card holder information
World Economic Forum Cyber Risk Framework (WEF-CRF)	The World Economic Forum	2015	All IT function, Information security, Risk	Risk based approach to cybersecurity, easily implemented	High-level document
ENISA	European Union Agency for Network and Information Security	Regular	All IT function, Information security, Risk	Source for information security recommendations, security resources for SMEs	Focus on security recommendations and publications for organisations
ITIL (Information Technology Infrastructure Library)	Central Computing and Telecommunications Agency	2011 (2018 scheduled update)	IT service management, IT processes	Management of internal processes, globally accepted, easy fit for all organisations	High level documentation, lacking specific details for implementation

The NIST cybersecurity framework provides a risk-based approach for organisations to address the effect of security risks from several domains (physical systems, cyber systems and people) and aims to reduce and better manage these risks (NIST, 2018). NIST suggests that organisations complement their framework with other security standards such as ISO 27000 that include security management processes for best practice. WEF-CRF is a risk-based framework similar to NIST as shown in Table 1. It provides the management with a high-level holistic approach (governance perspective) on cyber risks assessment and focuses on cyber resilience (World Economic Forum, 2015, 2018).

The PCI DSS is a unique standard. It was developed to provide a baseline of technical and operational security requirements to protect cardholder's data in card processing payments (PCI-DSS, 2016). The PCI DSS requires additional information security enhancement to assess and manage organisational information security risk (Al-Ahmad and Mohammad, 2013).

COBIT and ITIL are processed-based security frameworks. ITIL consist of libraries of best practices for managing information technology service and support delivery (Marrone et al., 2014). COBIT on the hand focuses IT governance best practices, that is defining and developing IT control requirements (Susanto et al., 2011). As process-based frameworks, ITIL and COBIT require organisations to implement the full framework to avoid gaps in the IT management processes (Marrone et al., 2014; De Haes et al., 2015).

ENISA focuses on the security of information within European member states by issuing publications on information security related topics and paying close attention to SMEs security (Antonucci, 2017). Similar to ENISA, SANS top 20 issues a high-level list of widely adopted security control which serves as a starting point for organisations when formulating ISPs (SANS, 2018).

The ISF standard of good practice for information security issued an integration of several aspects of information security management from a business perspective into a single comprehensive document (ISF, 2016). The IT-CMF:ISM presents a holistic business approach to information security; the primary audience is organisational management with a focus on improving IT capabilities using a maturity model concept (Innovation Value Institute, 2016; Antonucci, 2017).

The application of information security standards and frameworks in creating a security policy without a focus on the quality and content of the security policy may lead to a false sense of organisational security (Siponen, 2006). An effective security policy requires an assessment of the business risk appetite, management support, and employee compliant behaviours (Singh et al., 2013). However, SMEs are usually less aware of the information security standards and frameworks that will enable them to meet their business objectives and needs.

2.4.2 Information security and BYOD policy

A security policy is a formal document that outlines specific requirements or rules that must be met regarding the protection of the organisation's information asset and network (SANS, 2016b). Organisations need to create security policies to guide employee security behaviours such as procedures for accessing confidential/sensitive information, and use of social media, cloud storage, internet of things (wearables and smart devices), BYOD, third-party and partners access to information assets (Antonucci, 2017).

Organisational security policies should include anyone who has access to an organisation's information including third parties and employees with anywhere working arrangements. Security policies require a mix of the technical, non-technical, management and human aspects of the organisation's security system to be effective (Blount, 2015b; Singh et al., 2013). Management should be aware that security risks may arise from employees' actions relating to the use of BYOD when working from multiple locations. An information security breach from an employee's behaviour while working could significantly impact the business (Soomro et al., 2016).

Management should define how employees use BYOD for work tasks by creating or incorporating a BYOD policy into their ISP. NIST defines a BYOD policy as a security policy which specifies the organisation's assets that may be accessed via mobile devices (NIST, 2013). The flexibility of mobile technologies with access to the internet has become a preferred medium for employees to perform work tasks and maintain personal social interactions (Middleton et al., 2014). Crossler et al. (2014) observed that despite the acknowledged security risks associated with BYOD adoption, some organisations only specify basic controls to mitigate potential risks.

Employee compliance with security policies is important for managing security risks, yet prior studies have shown that it not always the case (Crossler et al., 2014; Zahadat et al., 2015). Therefore, we need a more comprehensive understanding of employee compliance with security policies to prevent information breaches, including the factors that influence employees' security behaviours.

2.5 Information security behaviour

The security of information systems has progressively shifted from a purely technical perspective to incorporate the human element of security management. Regardless of security policies and sophisticated security solutions, employees still fall prey to social engineering or unintentionally perform actions that could lead to unauthorised access and a security breach (Guo et al., 2011; Rocha Flores and Ekstedt, 2016). The inadequacies of technical security solutions and systems in preventing information breaches have led to research focused on the human as a part of the security solution (Furnell and Clarke, 2012).

Scholars are calling for more studies to determining factors that could influence or cause and individuals to change their security behaviours (Crossler et al., 2013; Johnston et al., 2015). The continuous transformation in the workplace such as the use of BYOD and anywhere working has made security a moving target, threats are evolving, and attackers are constantly seeking to exploit new vulnerabilities in employee security behaviours (Akhunzada et al., 2015). This study investigates the influence that mobile computing (BYOD), anywhere working and the reliance on smart technology for daily communications among other trends, has on the information security behaviours of SME employees.

Information security studies that have been carried out within organisational contexts investigating employee security behaviours have shown that personal belief (Bulgurcu et al., 2010) and the perception of one's capability (self-efficacy) (Ifinedo, 2012) positively influence employee's security intention. Studies that examine personal security behaviours of technology users (Anderson and Agarwal, 2010; Johnston and Warkentin, 2010) found that a combination of psychological, social, cognitive and fear components influence their security-related behaviours. Sommestad et al. (2015) suggested that variations of results may occur in studies possibly because of measurement methods, the operationalisation of constructs, mediating variables or sampling frames. For example, Ifinedo's (2012) study reported that an employee's assessment of a threat (perceived vulnerability) would positively influence his or her security behavioural intention, but Vance et al. (2012) found a negative influence. Thompson et al. (2017) found that prior experience strengthened the assessment of a threat in personal security and influenced security intentions. The inconsistencies observed in these studies may arise from the sample frame (employees and home users), because the threat may be perceived differently by each group. However, within the organisation, perceived vulnerability of a threat will influence employees security behaviours if they believe information assets are susceptible to threat (Ifinedo, 2012) but will not increase security intention where employees believe they are not subjected to security threats (Vance et al., 2012). Johnston et al. (2015) suggest that researchers should further investigate assumptions behind the threat perceived by studying different security contexts.

Behavioural information security research has examined why employees behave differently when accessing or using information systems when working from the office. Studies divided employee security behaviours into three categories. The first category consists of individuals who intentionally sabotage information systems, often labelled as deviant behaviours (D'Arcy et al., 2009; D'Arcy and Devaraj, 2012; Willison et al., 2016). The second category is individuals who unintentionally cause damage to information systems by using a weak password, carelessly clicking on phishing emails links or being noncompliant with security policies (Guo et al., 2011; D'Arcy et al., 2014b). The final category is individuals who are security conscious and protect information assets by following appropriate security procedures and best practice (Burns et al., 2017; Posey et al., 2015). Practitioners and scholars have found that employees in the second category remain the top source of security threats to organisational information assets (D'Arcy and Lowry, 2017; PWC, 2018). It is beneficial to understand factors that influence these employees' behaviours and guide organisational management, especially SMEs, and steps that could be taken to encourage positive security behaviours.

Prior studies have considered rational and non-rational factors that influence employee security behaviours. Rational decision making in information security research, suggests that an individual's security behaviour is determined by the costs and benefits of options available (Bulgurcu et al., 2010; D'Arcy and Lowry, 2017). The major assumption of these studies is that the decision to engage in a security behaviour originates from a rational decision process. However, employees may unconsciously make irrational decisions when working which requires less effort, such as not updating a security password regularly for ease of remembrance (Guo, 2013).

Scholars have applied fear appeals within the information security context to examine behaviour change. A fear appeal is a persuasive message or circumstance that include the element of threat to a subject (Johnston and Warkentin, 2010). Findings suggest that when individuals perceive a threatening circumstance, their rational decision process leads to a change in their behaviour (Ifinedo, 2012; Johnston et al., 2015; Thompson et al., 2017). Different aspects of the fear appeal significantly affect the cognitive process that causes individuals to change behaviour such as response cost (Thompson et al., 2017), response efficacy (Ifinedo, 2012; Johnston et al., 2015; Menard et al., 2017). Some studies suggest that employees employ neutralisation techniques to rationalise their behaviour (Siponen and Vance, 2010; Willison et al., 2016). Employees who unintentionally engage in insecure behaviour practices or do not comply with security policies when working could apply neutralisation techniques, such as failing to encrypt documents because it takes too long, to justify and rationalise their actions (Siponen and Vance, 2010). Decision-making processes are not always rational. D'Arcy and Lowry (2017) discovered that the inclusion of affect, an individual's state of feeling, as a key aspect of rational decision-making, could influence employee security behaviours. In the context of information security, the individual's response to threats of a data breach may not follow a rational decision-making process to protect organisational information assets, because threats presented may or may not involve the individual directly (Menard et al., 2017).

Some studies have focused on non-rational factors that could influence employee security behaviours. Pahnila et al. (2007) and Vance et al. (2012) included habit's influence in their study on employees' intention to comply with ISPs. Vance et al. (2012) showed that habit as a form of automatic behaviour could influence an employee's decision to comply with security policies. Similarly, Pahnila et al. (2007) found that habit had a significant effect on employees' behavioural intention to comply with security policies. Very few studies in information security have examined the influence of employees' past behaviour or habit on security behaviours. In this study, habit is included to examine SMEs employee security behaviour when working from anywhere using BYOD.

Organisational stress research has found links between work stress and employee behaviours. Technostress is a term used to describe an individual's stress from their inability to cope or deal with ICT use in the workplace (Ayyagari et al., 2011). Anywhere working employees have to manage stress resulting from the use of technology and deal with the complexities of security procedures when accessing information assets from multiple locations when technical support is not available (Bayrak, 2012). D'Arcy et al. (2014b) examined employee security-related stress (SRS) as a form of psychological stress caused by information security-related demands resulting in cognitive overload or exhaustion of one's cognitive abilities. For example, employees may encounter information security stress when precious work time is spent requesting access to information or software and waiting for IT personnel to set up security access or follow a self-installation process before accessing resources. Studies found that employees coped with SRS by rationalising and justifying noncompliant behaviours and negative security actions when working (D'Arcy et al., 2014b).

Lee et al. (2016) examined factors that could lead to employee information security stress and found that work overload that is extra work as a result of information security could lead to employee stress. The literature on workplace stress resulting from technology (Tarafdar et al., 2007; Ayyagari, 2012; D’Arcy et al., 2014a) reveals that there are consequences to the organisation when employees experience technology stress such as IT misuse which could lead to serious information security risks. D’Arcy et al. (2014b) and Lee et al. (2016) study show that organisations need to understand the impact of information security stress on employees. However, there are few empirical studies on SRS that investigate the multidimensional impact of SRS. Studies on stress show that work impediment has a significant influence on employee’s attitude towards ISP (Bulgurcu et al., 2010; D’Arcy and Lowry, 2017). Work impediment refers to setbacks to an employee's daily tasks and activities resulting from compliance with the requirements of the ISP (Bulgurcu et al., 2010). Employees in SMEs may encounter techno-security-stress when working from anywhere using BYOD.

Previous studies have investigated factors such as stress, fear, and work impediment as negative factors that influence employee security behaviours. Posey et al. (2015) assessed positively motivated security behaviours and discovered that organisational commitment influenced employees to personalise organisational threats and respond with protective behaviours. Burns et al. (2017) integrated psychological capital (PsyCap) in their study to understand the change in an employee’s behaviour to protect organisational information assets. PsyCap is an individual’s expectation of things to go their way and the general belief that good rather than bad things to happen (Burns et al., 2017). The assessment of employees’ PsyCap in the study regarding information security protective behaviour, suggests that a strong relationship exists between an employee’s PsyCap and protective behaviours (Burns et al., 2017). However, PsyCap levels are subject to increase or decrease depending on factors surrounding the employee such as their work context or personality traits (Peterson et al., 2011).

Personality traits have been used to explain individual’s behaviour outcomes. Bansal et al. (2010) showed that an individual’s disposition, as an intrinsic factor, impacts their online behaviour in regards to their trust and the disclosure of sensitive information. Personality traits research outline several kinds of personalities which include the Goldberg’s Big Five: openness, conscientiousness, extraversion, agreeableness and neuroticism; Machiavellianism, social desirability, among others. In the context of information security, personality traits have been used to understand behavioural intention towards information systems security. Kajzer et al. (2014) used seven personality traits (the Big Five, Machiavellianism, and social desirability), to show that different personality traits respond differently to security awareness and messages.

Shropshire et al. (2015) examined two kinds of personality traits (conscientiousness and agreeableness). The findings from the study showed that both traits had a significant impact on the relationship between intention and behaviour. Responding to the call for more studies on personality trait in different contexts (Herath and Rao, 2009; Kajzer et al., 2014); this study examines the influence of hardiness personality traits on SMEs employees when working from multiple locations using BYOD.

Psychologists have examined why certain individuals respond better to stressful life events than others. One key finding was the personality trait hardiness. Hardiness is a constellation of personality characteristics that function as a resilience resource in the encounter with stressful life events (Kobasa, 1979). Hardy individuals possess three major characteristics/attitudes: commitment, control, and challenge disposition which enable them to adapt to stressful life events (Kobasa et al., 1982). Individuals with a hardy disposition have a general sense of purpose or meaning (commitment), they see change not as a burden but as a normal aspect of life (challenge), and feel that they can influence life events (control) (Funk and Houston, 1987).

Hardiness has been studied extensively in numerous fields. Bartone (Bartone, 2006; Bartone et al., 2012, 1989) studied hardiness as a stress buffer in military leaders and officers. Findings showed that hardy military leaders facilitated hardiness among the groups they coordinated making group members more resilient when exposed to work-related stressors (Bartone, 2006). Bartone (2012) acknowledged that today's modern organisations consist of technologies that could inherently lead to stress, but a hardy person stays courageous in the face of new experiences as well as disappointments.

Anywhere working employees performing work tasks with BYOD may experience different situations and security threats that could lead to stress when working from multiple locations. The commitment disposition in hardiness was found to reduce threat appraisal and make individuals mentally stay in the threatening situation and confront its demands and consequences (Florian et al., 1995). This study integrates hardiness as a psychological resource that may positively influence employees' security behaviours especially among SMEs employees who work from anywhere using BYOD.

The literature reviewed in this chapter shows the variables from several theories that scholars have examined to determine the factors that may cause employees to change their security behaviour. This study will draw on some of these variables from the theories used in previous studies to investigate how SME employees perceive security behaviours. The next section discusses the relevance of having SMEs adopt, create and comply with security policies and regulations.

2.6 Small and medium-sized organisational context of information security

The economic growth of a nation is measured using various indicators, one of them is the number of SMEs. SMEs are defined differently, depending on the country, using criteria such as size (number of employees) or annual turnover. In Australia, SMEs are businesses with 0 – 199 employees and account for over 50% of businesses in the country, as partners and suppliers of goods and services (Australian Bureau of Statistics, 2017). In the United States of America (USA), about 99% are SMEs businesses with 0 – 999 employees, employing almost half of the working population (Office of Advocacy, 2017). In the United Kingdom, 99% of businesses are SMEs with less than 250 employees and employing about 60% of the working population (Department for Business, Energy & Industrial Strategy, 2017). These statistics highlight the important role of SMEs in the supply chain network and the growth of a nation's economy.

Information security and data breaches/attacks target SMEs especially those who carry out transactions over the internet. A recent security threat report showed that in 2017 there was a 200 per cent increase in supply chain malware attacks when compared to previous years (Symantec, 2018). Studies carried out on SMEs show that they usually have resource constraints (human and financial capital) forcing them to focus available resource on immediate issues (Street et al., 2017). This constraint potentially influences SMEs attitude and investment towards information security management. Kurpjuhn (2015) reported that SMEs take advantage of modern technologies trends such as the use of BYOD and encourage their employees to work from anywhere to gain competitive advantages. Nguyen et al. (2015) found that SMEs are more customer oriented which drives investment in IT solutions to improve the customer relationship and satisfaction.

SMEs underestimate the security risk their employees may encounter when working due to wrong perceptions based on their size (Ng et al., 2013; Renaud, 2016). Due to their small size and resources, SMEs are inclined to use open source and free security solutions available from vendors (Mansfield-Devine, 2016), potentially giving them a false sense of security. Ng et al. (2013) found that some SMEs collaborating with large organisations rely on their collaborators for security against information breaches. Hackers are aware of SMEs security shortcomings as they encounter less resistance when trying to compromise information assets and systems. The shift of attacks from large organisations to SMEs calls for information security researchers to examine SMEs employees' security behaviours and understand factors that could influence their behaviour when working from anywhere using BYOD.

The focus of this study is to examine the perception of SME employees towards security behaviours. That is SME employees who unintentionally misuse information systems or do not comply with security policies when working from multiple locations using BYOD. These individuals are usually insiders (including third-parties) with access to information assets, they pose serious threats (Wang et al., 2015) and account for most of the breaches that occur within organisations (Cheng et al., 2017).

2.7 Summary

This chapter examines technology and work trends which have introduced new areas of security risks for SMEs. Hackers are exploiting weaknesses in human behaviour and target SME employees to gain easy access to information assets and supply chain networks. This shows the need to understand the security behaviours of SMEs employee and factors that may influence employee behaviour when working from anywhere using BYOD. The next chapter discusses the theoretical framework and presents the theoretical model.

Chapter 3: Theoretical Framework

3.1 Introduction

This chapter presents the theoretical framework used to investigate the factors that may influence employee security behaviours when working from multiple locations. First, an overview of theories used in information systems security studies is presented. Next, a discussion of the theories and the components adapted to create the theoretical model to explain how employees' perceive security behaviours. The chapter concludes by presenting the theoretical model for the study.

The literature review in the previous chapter showed that there is limited understanding of the security behaviours of employees working in SMEs. In 2017, the rate of information breaches among SMEs increased significantly compared to previous years. Lack of security knowledge was one of the reasons for this increase (NZ Herald, 2018). This study examines factors that may influence SME employees' security behaviours. Human security behaviour is complex and influenced by factors from the environmental, social, and personal perspectives. Information security studies have employed theories to investigate and examine the information security behaviour of employees (Moody et al., 2018).

3.2 Theories in information systems

Researchers in information systems (IS) have used various theories in their study to understand, explain, and predict security behaviours. Information and Communications Technology (ICT) has become an integral part of society, changing the way people work, transact business, interact and live. Organisations set up procedural (such as security policies) and technical countermeasures (such as authentication systems) to reduce employee IS misuse and protect information assets (D'Arcy and Hovav, 2009). IS scholars have borrowed theories from other disciplines such as criminology, psychology, sociology, health, to understand factors that motivate and influence employee's security behaviours (Moody et al., 2018). The multidisciplinary nature of IS studies allows researchers to adopt theories from different disciplines to understand security behaviours.

From 2000 onwards, studies in information security behaviours have applied deterrence theory to understand and prevent negative employee behaviour towards IS (D'Arcy and Hovav, 2009; Herath and Rao, 2009; Siponen and Vance, 2010). More recently, scholars employed the theory of reasoned action/planned behaviour to examine individual's abilities and environmental factors (such as social influence) that may affect employee security behaviours (Bulgurcu et al., 2010; Guo et al., 2011; Ifinedo, 2014). Information security researchers have also used the protection motivation theory to examine individual's cognitive processes which led users to either perform or not perform positive or negative security behavioural actions (Woon et al., 2005; Johnston and Warkentin, 2010; Ifinedo, 2012; Vance et al., 2012). While some of these studies use a single theory (for example Posey et al., 2015), other studies used more than one theory to examine and understand employees' information security behaviours (Cheng et al., 2013; Ifinedo, 2014).

Recent changes in the threat landscape call for better understanding of employee's emotional and cognitive resources that influence expected security behaviours even when working in an unfavourable security environment (Pham et al., 2017). The next section explains each of the theories and the main constructs used to develop the theoretical framework for this study.

3.2.1 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) (Ajzen, 1985) in social psychology is a revised version of Fishbein and Ajzen's Theory of Reasoned Action (TRA) which shows the causative sequence of beliefs, attitude, social norms and intention that leads to a projected behaviour. The TPB extends the TRA by including perceived behaviour control (PBC) as an independent determinant of behavioural intentions (Ajzen, 1991). In the TPB, behavioural intention which in turn predicts behaviour is influenced by the interrelationship of attitude, subjective norms and PBC (Al-Suqri and Al-Kharusi, 2015). Attitude refers to the favourableness or unfavourableness of engaging in a specific behaviour (Fishbein and Ajzen, 1975). Subjective norms are the perceived social pressure the individual encounters to perform or not perform the specific behaviour (Ajzen, 1991). PBC refers to the individual's belief in their ability to perform the desired behaviour (Ajzen, 1991). Ajzen (1991) theorised that if intentions are strong enough to influence behaviour, the more likely it is for the behaviour to be performed.

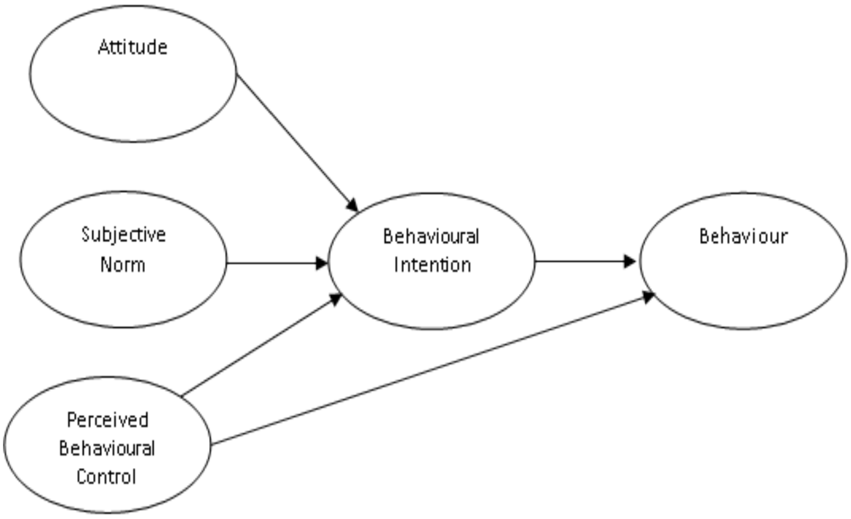


Figure 1: The theory of planned behaviour (Ajzen, 1985)

Information security scholars have attempted to understand why some individuals within the same organisation portray different behaviours towards security policies. Using the TPB, previous studies have evaluated workers behaviour based on behavioural beliefs, normative beliefs, and self-efficacy as antecedents of attitudes, subjective norms, and perceived behavioural control (Bulgurcu et al., 2010). Bulgurcu et al. (2010) combined TPB with other variables and revealed that all three constructs (attitude, normative beliefs, and PBC as self-efficacy) used in the research model had a significant effect on employee's intention to comply with security policies. Safa and von Solms (2016) applied the TPB to study information security knowledge sharing among employees. Findings from their study showed that by linking attitude, intention and behaviour to sociological motivators like reputation or promotion, employees' intention to share information security knowledge is positively influenced (Safa and von Solms, 2016).

The TPB constructs; attitude, subjective norms and PBC emphasises the controlled aspects of information processing and decision making processes in individuals (Ajzen, 1991). Ajzen (2011) suggested that other factors such as social support or various background factors can be accommodated within the theory to provide a better understanding of human social behaviour. Some scholars have criticised TPB for being too 'rational' because human judgements and behaviour are usually mediated by cognitive bias that influences the behaviour exhibited (Ajzen, 2011). In this study, *subjective norms* are adapted from TPB to capture social influences employees may encounter (from colleagues or friends) that may cause them to change their security behaviour, especially when using BYOD. *Attitude* towards an expected behaviour and *intention* to perform the expected behaviour are adapted from the TPB to predict employee security behaviour.

Attitudes, subjective norms and *intentions* about the behaviour performed are assumed to be guided by the individual's cognitive effort (Ajzen, 2011). The insufficiency of the TPB to fully understand the individual's cognitive capacity that could influence behavioural intention led to the integration of the protection motivation theory to address this gap.

3.2.2 Protection Motivation Theory

Protection Motivation Theory (PMT) was developed by Rogers (1975) originally to understand the relationship between fear appeals and change in behaviour as a response to the fear. Fear appeal refers to the content of communication describing an unfavourable consequence from failure to adopt a given recommendation (Rogers, 1975). PMT uses the expectancy-value theory and cognitive mediating process to understand what motivates an individual to carry out a recommended behaviour to protect themselves in response to threats (Floyd et al., 2000). The cognitive mediating process in the protection motivation model consists of two appraisal processes: threat appraisal and coping appraisal that could lead to either an adaptive or maladaptive response (Rogers, 1983). The threat appraisal refers to how the individual assessment of the threatening circumstance, made up of perceived vulnerability (likelihood of being at risk to the threat), perceived severity (consequences of the threat) and an intrinsic or extrinsic rewards that would follow a maladaptive behaviour (not to protect self or others) (Rogers, 1983; Ifinedo, 2012; Menard et al., 2018).

The coping appraisal pertains to the ability of an individual to cope with or avert the perceived threat (select an adaptive behaviour) (Rogers, 1983; Floyd et al., 2000). The coping appraisal process factors are self-efficacy (the ability to carry out the adaptive response), response efficacy (the belief that the adaptive response will work) and response cost (costs associated with taking the adaptive response) (Floyd et al., 2000). An individual's intention to engage a protection motivated behaviour will result from the cognitive appraisal process, if an individual positively evaluates the response efficacy and self-efficacy, while higher response costs will lead to lower protection motivation (Sommestad et al., 2015).

PMT has been used to study how fear motivates individuals to take on protective behaviours when they feel threatened. PMT was originally used in health-related studies to persuade individuals to choose healthy lifestyles, reduce alcohol use and prevent disease acquired from previous bad health behaviours (Boer and Seydel, 1996). In the information security context, employees' understanding of the severity of the threats influences their information security behaviours (Herath and Rao, 2009). In this study, the aim was to examine if the perceived vulnerability and severity of threats from multiple work locations, the work tasks or the use of BYOD would cause an employee to change their security behaviours.

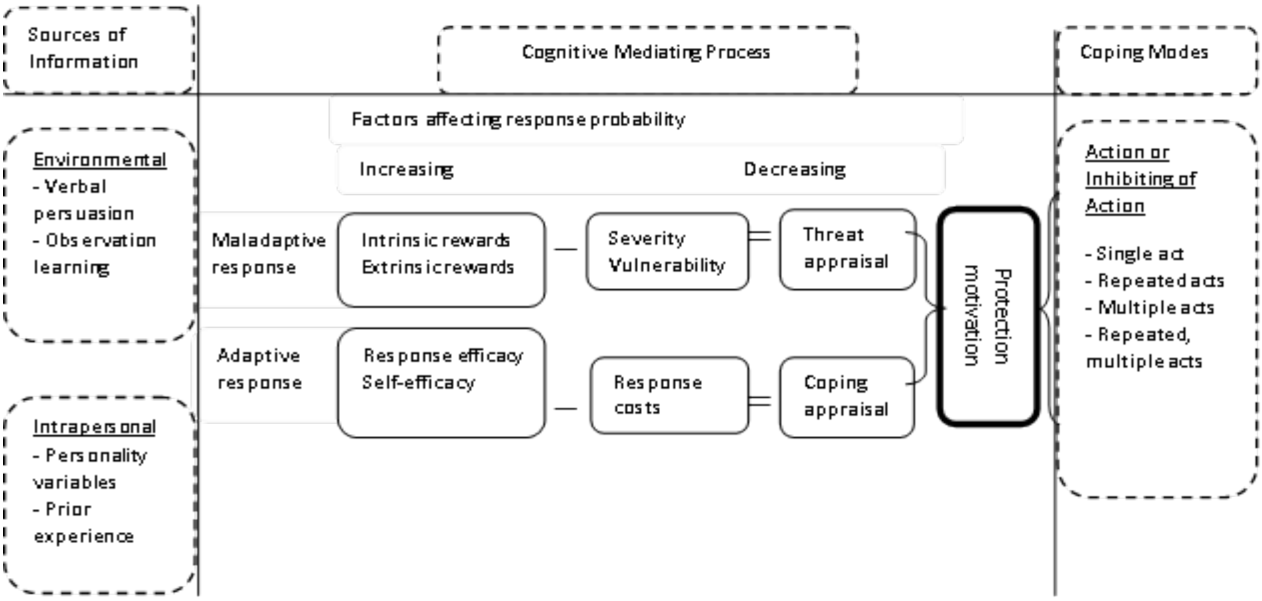


Figure 2: Schema of protection motivation theory (Rogers, 1983)

Johnston and Warkentin (2010) proposed a fear appeal model that showed a user's intention to engage in a security action is socially influenced along with self-efficacy and response efficacy, as a direct antecedence of threat severity and susceptibility. The addition of social influence enabled the researchers to understand the participant's intentions to accept the use of security technology (Johnston and Warkentin, 2010). Although fear appeals serve as a good predictor of intentions to exhibit a protective behaviour, some information security researchers have integrated two or more theories or introduced other variables into PMT to produce better behavioural predictions (Ifinedo, 2012; Burns et al., 2017).

The inclusion of psychological ownership to PMT in Anderson and Agarwal's (2010) study significantly influenced home users intentions to perform security-related behaviours. Herath and Rao (2009) integrated PMT, deterrence model, organisational commitment, and Taylor-Todd's decomposed theory of planned behaviour (TPB), and found that employees have a positive attitude toward security policies if they are concerned about a security threat. In another study, Ifinedo (2012) integrated PMT and TPB. The study discovered factors that influenced employees' intention to comply with information security policies in organisations (Ifinedo, 2012).

In an exploratory study, Siponen et al. (2014) fused components of PMT, TRA and cognitive evaluation theory to understand why employees are non-compliant to security policies. The results showed that fear appeals influenced employees' behavioural intention to comply with security policies. Thompson et al. (2017) extended PMT in their study and found that the personalisation of threats influences personal security behaviours of home computer users and mobile device users differently.

In PMT, the cognitive mediating process which causes an adaptive or maladaptive behaviour when an individual encounter a threat situation, arises from stimuli or information sources outside of the human cognition that may influence behaviours. There are factors that PMT does not capture. Rogers (1975) advocated that researchers could improve the prediction of protective behaviours by including additional variables and broaden the understanding of fear appeals. The cognitive process which triggers a protective behaviour is sometimes mediated by intrapersonal variables (Rogers, 1983) such as emotions, social attitude or past behaviours. This study adopts the threat appraisal variables, *perceived vulnerability* and *severity*, to understand employees' security intention to engage in security behaviours when working from multiple locations using BYOD.

PMT does not capture all sources of information that could affect the employees' cognitive process and influence their security behaviours when they perceive threats. Habit is included in the model to capture past behaviours that could influence the employees' security intention.

3.2.3 Habit

Habit is included in the theoretical model to understand how past behaviours that may affect the employees' cognitive mediating processes and influence their security behavioural intention. Human behaviour is formed from repeated everyday activities. Ajzen and Fishbein (2000) examined the role of habit in human behaviour, showing that frequently performed behaviour leads to the formation of a habit which later controls cognitive mediation and behaviour. Habits are learned from a sequence of acts that have become automatic responses to specific cues (Verplanken and Aarts, 1999). The debate on habit and habit formation in behavioural studies led to Verplanken and Aarts (1999) study on the strength of habit in planned behaviour and rational decision-making. The study revealed that habits influence cognitive orientation, making individuals pay less attention to new information and courses of action (Verplanken and Aarts, 1999). Individuals mentally associate the stimulus with an automatic-cue for action. Habitual response occurs when a similar stimulus is presented to an individual (Orbell and Verplanken, 2015).

Habit as a form of routinized behaviour is often assessed by measures of frequency of past behaviour. Verplanken and Orbell (2003) criticised this view arguing that behavioural frequency of a habit does not determine future behaviour but rather it is the automaticity of responding to certain cues. Verplanken and Aarts (1999) developed and validated an instrument to measure the automaticity of habit as a psychological construct to address the measure of behavioural frequency estimation.

There have been a few studies on the role of habit in IS usage behaviour. Cheung and Limayem (2005) studied the effect of habit on the relationship between intention and IS usage behaviour. The study showed that the stronger the effect of habit, the weaker the effect of intention on continued use of the information system. Limayem et al. (2007) found that habit moderated the relationship between intention and continued IS usage behaviour. Other studies examined the direct effect of habit on intentions to use information technology (IT). Ortiz de Guinea and Markus (2009) showed that habit plays a role in the continuous use of IT to perform tasks.

In behavioural information security studies, there are few research on the effect or role of habit on security behaviours. Pahnila et al. (2007) studied habit to investigate how employees' compliance with security policies can be improved. Findings from the study showed that habit had a significant effect on intention to comply with information security policies. Vance et al. (2012) showed that habit significantly influences an individual's cognitive mediating process and strengthens their security intentions. These studies demonstrate the strength of habit as a determinant of employee security behaviour.

Responding to Moody's et al. (2018) call for more research to examine habit in different types of information security behaviours, habit is included as a construct in this study. The theoretical model measures the strength of *habit* and its influence on SME's employees' security intentions and predicts their security behaviours. The next section discusses hardiness as another variable included in the study.

3.2.4 Hardiness

Studies in psychology have shown that stress occurs when a life event demands a readjustment of an individual's normal routine (Kobasa, 1979). In the previous section, habit is portrayed as a routine; stress arises when an event interrupts an individual's routine making them to adapt or learn a new routine. Psychologists have predicted a relationship between stress and illness or health. However, Kobasa (1979) observed that some individuals adapted well in a highly stressed situation. Hardiness is a term used to characterise individuals who respond or adapt better than others to high degrees of stress. Hardy individuals possess three personality dispositions; commitment, control and challenge. The commitment disposition is expressed as a tendency to be involved in a situation allowing the individual to identify purpose and meaning in events, things and persons in their environment (Kobasa et al., 1982). The control disposition is expressed as a tendency to influence rather than feel helpless in a stressful event, by increasing the likelihood that events are natural outgrowth of one's action and not foreign and overwhelming experiences (Kobasa et al., 1982). The challenge disposition mitigates the stressful events when the individual view them as stimulating rather than threatening, causing them to make the required readjustment (Kobasa et al., 1982). These three dispositions are interrelated and constitute positivity and resiliency in a hardy individual when facing high degrees of stress in life (Maddi and Khoshaba, 1994).

Early studies have shown positive results of hardiness on performance among different sample groups; management personnel (Kobasa, 1979; Kobasa et al., 1982), students (Maddi et al., 2006) and military officers (Bartone, 2006; Bartone et al., 2008, 1989). Findings from these studies suggest that individuals with high levels of hardiness performed better despite the stressful condition of work, study and harsh military conditions. Pioneer studies on hardiness sought to explain why some highly stressed individuals had better health condition and performance than others (Bartone, 2006; Kobasa, 1979), no study was found so far to examine the effect of hardiness personality trait on security behaviours.

Previous research highlighted the positive impact of hardiness. This study has included *hardiness* (*commitment, control* and *challenge*) in the theoretical model to help better explain security behaviours. Security-related stress is included in this study to understand the effect of hardiness on employees' security behavioural intention when working in stressful conditions.

3.2.5 Technostress

The final factor relevant to the study of SMEs employees' security behaviour when working from multiple locations using BYOD is technostress. Technostress is the negative impact on an individual's attitudes, thoughts, and behaviours caused either directly or indirectly by ICT (Riedl et al., 2012). Some studies have shown the difficulty of giving ICT support to employees working from multiple geographical locations (Bayrak, 2012). Anywhere working employees require organisational support such as managerial guidance, to reduce psychological strain/stress and enhance their work performance and wellbeing (Bentley et al., 2016). Ayyagari et al. (2011)

studied technology characteristics (such as usefulness, complexity, reliability) which could influence stressors (events encountered such work task) and lead to stress. Findings from the study of working professionals showed that constant connection to IT devices increases employee workload, leading to stress (Ayyagari et al., 2011).

Related studies on technostress within the organisation suggest that technology usage changes human behaviour negatively leading to reduced job satisfaction, less organisational commitment and intention to stay with the organisation (Ragu-Nathan et al., 2008). Tarafdar et al. (2007) study of users in 223 organisations found that technostress arising from the fear of technology uncertainty was positively related to role stress and work overload affecting individual productivity. Riedl et al. (2012) investigated technostress using a laboratory experiment. Results from the study showed that cortisol (a major stress hormone in humans) increased significantly when the users experienced difficulty in the human-computer interaction task. These studies show that technostress can have negative results, such as causing a change in user's attitude and behaviour.

In behavioural information security, D'Arcy et al. (2014b) posited that similar to technostress; employees may experience security-related stress (SRS) when information security requirements increase workload and create added time pressure when performing work tasks. Findings from the study showed that stressful security requirements could lead to employee rationalisations of security violations, which in turn leads to negative security behaviours (D'Arcy et al., 2014b). Technostress is integrated into the theoretical model to investigate whether techno-security *stress* encountered when working with BYOD from multiple locations will influence employees' *attitude* towards security and change their security behaviours.

3.3 Theoretical model

Figure 3 depicts the theoretical model developed for the study. Table 2 provides definitions for the constructs used in the model adapted from habit, TPB, PMT, hardiness and technostress. TPB posits that *attitude* towards a behaviour is influenced by behavioural beliefs that are, background factors. In the theoretical model, *hardiness* and *technostress* are factors that may positively or negatively influence an employee's *attitude* towards security behaviours. *Intention* to carry out a security behaviour is influenced by the *attitude* towards the behaviour and *subjective norms* such as social relationships with work colleagues and friends. Perceived threats may lead individuals to adjust their behaviour depending on the perceived risk of the circumstance; threat appraisals may positively influence security intentions and predict security behaviours.

Table 2: Definition and sources of constructs

Construct	**Definition**	**Sources**
Hardiness	Hardiness is a constellation of personality characteristics that function as a resource to resist stressful life event	Hardiness theory (Kobasa, 1979)
Commitment	A tendency to feel involved in life's activities rather than experience alienation	Hardiness theory (Kobasa, 1979)
Control	The belief that events experienced can be controlled or influenced	Hardiness theory (Kobasa, 1979)
Challenge	The tendency to see change as a normal aspect of life rather than as a threat and as an opportunity for growth	Hardiness theory (Kobasa, 1979)
Stress	The overall transactional process caused by ICTs and security requirements	Technostress (Ayyagari et al., 2011; D'Arcy et al., 2014)
Attitude	The degree to which a person evaluates or appraise performance of the behaviour in question	Theory of planned behaviour (Ajzen, 1991)
Subjective norms	The perceived social pressure to perform or not to perform a behaviour	Theory of planned behaviour (Ajzen, 1991)
Perceived severity	The expectancy of a threat to one's person (that is bodily harm)	Protection motivation theory (Rogers, 1983)
Perceived vulnerability	The expectancy of being exposed to a threat	Protection motivation theory (Rogers, 1983)
Habit	Learned sequences of acts that become automatic responses to specific cues, and are functional in obtaining certain goals	Habit (Verplanken and Aarts, 1999)
Intention	Motivational factors captured that assume to influence a behaviour	Theory of planned behaviour (Ajzen, 1991)

The measures of *habit* strength developed by Verplanken and Orbell (2003) are used to access the security habits. Verplanken and Aarts (1999) posit that when strong habits have developed, intentions may lose their predictive ability. In line with their study, *habit* is modelled to influence security *intentions*. In the TPB, Ajzen (1991) theorises that the stronger the *intention* towards a behaviour, the more likely the *behaviour* will be performed if there are enough motivational factors available. Prior studies on security behaviour take into account behavioural intentions with the assumption that intentions may or may not be carried out. The theoretical model includes a relationship between *intention* and *behaviour* to examine the extent to which SMEs employee's security intentions could translate to actual behaviour in line with previous studies (D'Arcy and Lowry, 2017; Thompson et al., 2017).

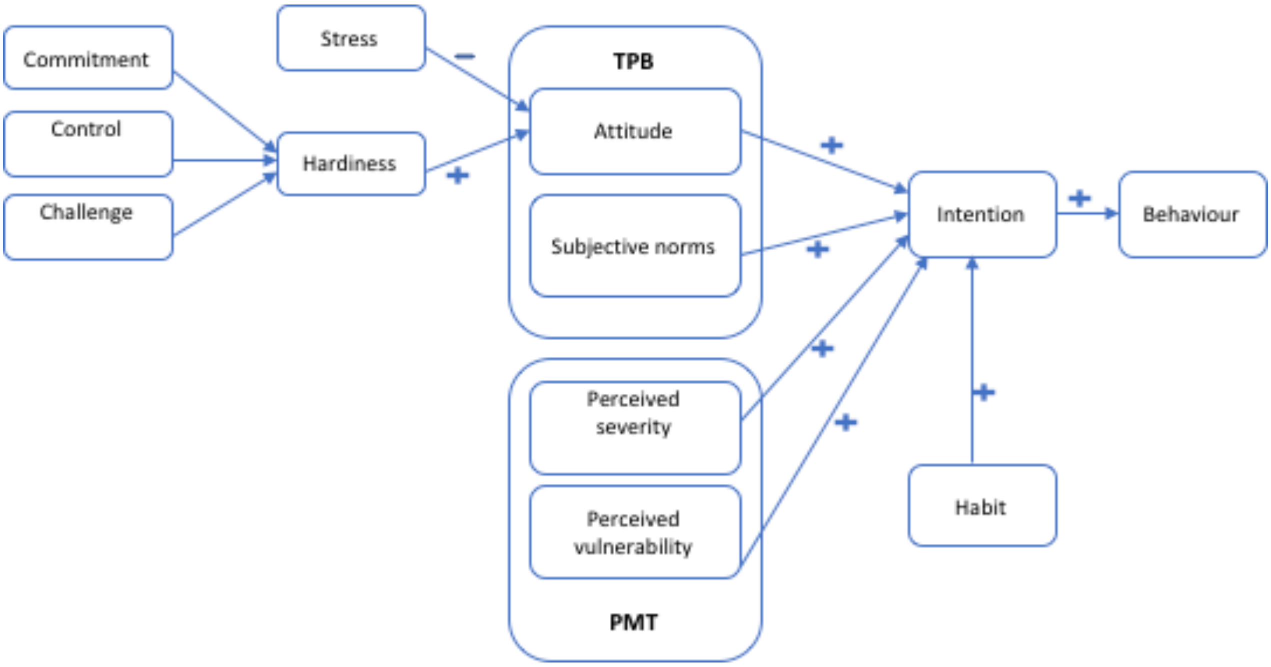


Figure 3: The theoretical model of SME employee security behaviour

3.4 Summary

This chapter presented the theoretical framework for this study. The theoretical model used to examine and understand the security behaviours of SME employees used variables from the TPB, PMT, habit, hardiness and stress. The next chapter discussed the research design and methodology of the study used to obtain the data used to test the theoretical model.

Chapter 4: Research Design and Methodology

4.1 Introduction

This chapter discusses the research design and methodology including the rationale for the methods selected in this study. The aim of this research was to investigate the security behaviour perception of SME employees when using their personal devices (BYOD) for work purposes from multiple work locations. A quantitative research design and method was used to explore the relationship between variables in the theoretical model.

A scenario-based survey was developed and distributed to participants recruited from an online crowdsourcing website to understand the factors that may influence the perception of security behaviours among SME employees. The quantitative data collected was used to answer the research question: *How do the type of work tasks and locations of work change SME employee security behaviours when using personal devices?*

4.2 Research design

A research design is a blueprint for the collection, measurement, and analysis of data (Sekaran and Bougie, 2013). There are three major research designs: quantitative, qualitative and mixed methods design. Quantitative research utilises a set of techniques such as surveys to collect and analyse numerical data and examine interactions between given variables usually to test or develop a theory (Recker, 2013). Qualitative research emphasises the collection and analysis of text data using techniques such as interviews, to understand a phenomenon in a context where little knowledge is available (Saunders et al., 2016). Mixed method research uses data collection and analysis techniques from both quantitative and qualitative methods (numbers and text) (Recker, 2013).

A quantitative research design was used in this exploratory study to understand the variables drawn from the theoretical framework discussed in the previous chapter. Exploratory research helps to clarify the understanding of an issue, problem or phenomenon (Saunders et al., 2016). This approach was chosen because previous research on behavioural information security on SMEs was limited. Therefore, an exploratory study was suitable to allow the researcher to gain insight into the security behaviours of SME employees and address the research aim.

4.2.1 Quantitative research method

Quantitative research emphasises quantities and numerical data. Methods of data collection in quantitative research include structured surveys. Survey data fall into three categories; self-completion (such as internet or mail surveys), interviewer-completed (similar to structured interview either face-to-face or via telephone), and observation studies (participants behaviour monitored or recorded into numerical format) (Hair et al., 2016). The survey design was a self-completed. This was appropriate because of the sensitive nature of information security studies (Kotulic and Clark, 2004).

In the information systems discipline, surveys are common because they are easy to administer, provide responses that can be generalised to the population and allows the researcher to determine the values and relations of variables and constructs (Newsted et al., 1998). Information security researchers have used several methodological perspectives to conduct their studies and utilised quantitative survey methods for data collection and analysis (Bulgurcu et al., 2010; Ifinedo, 2012; Thompson et al., 2017). Therefore, this study adapted constructs used in prior studies to develop the survey used to collect data.

The survey used hypothetical workplace scenarios to overcome the potential difficulty of self-reporting unethical behaviours (Pogarsky, 2004). Scenario-based surveys present the study participants with written hypothetical situations and ask about the likelihood that they would behave the same way under the same circumstances (Cheng et al., 2013; Siponen and Vance, 2014). The development of the workplace scenarios used in the study followed suggested guidelines from Siponen and Vance (2014).

The sample population for the study were employees of small and medium-sized organisations. The sample population refers to respondents representative of the general population involved in the data collection process (Recker, 2013). The participants were randomly selected with the criteria: over eighteen years of age, SME employee, use of BYOD for work and work from multiple locations.

To reach the target population for the study, data was collected from participants using Amazon's Mechanical Turk. Crowdsourcing platforms such as Amazon's Mechanical Turk, InnoCentive, or Crowdflower, offer researchers access to design surveys and distribute them to willing participants online for a fee (Bohannon, 2011; Steelman et al., 2014). These platforms offer a heterogeneous sample population, more extensive demographic and unique organisation features (such as SMEs) that could not be previously easily accessed (Lowry et al., 2016).

The next sections provide a comprehensive overview of the survey design, item development, scenario development, including the ethical considerations.

4.3 Survey design

The first section of the survey captured the demographics of the participants, including items such as gender, age, educational level, organisational size, availability and awareness of information security and bring your own device (BYOD) policy. The second section measured the respondent's general security disposition such as *attitude* and *hardiness*. The final section of the survey randomly presented one of four scenarios to each respondent to establish security behaviour.

All measurement items in the survey, except perceived realism, were assessed on a seven-point Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree). Perceived realism was a single item construct with the labels 1 (very unrealistic) to 7 (very realistic). The seven-point Likert scale was preferred because the majority of the survey items were adapted from studies that used similar scales (Ayyagari et al., 2011; Ifinedo, 2012; Thompson et al., 2017).

The survey was designed on the Qualtrics website because the University has an enterprise licence for the software. An account was created on Amazon Mechanical Turk (MTurk). A unique code was embedded into the Qualtrics survey to enable the researcher to match each response on MTurk to the Qualtrics response received.

4.3.1 Control variables

In the demographic section of the survey age, gender, years of work and organisational size were included as control variables in the model analysis. Prior behavioural information security research suggests that certain demographic characteristics (control variables) usually influence information security behaviours. For example, Anwar et al. (2017) showed that men exhibited better cybersecurity behaviours than women in the workplace.

4.3.2 Item development

All measurement scales used to develop the survey were taken from previously validated research. To improve the reliability of results in the study, the selection of questions for the survey followed the Straub and Boudreau (1989) guidelines to use previously validated and tested questions. *Subjective norms* and *attitude* were adapted from Ifinedo (2012) and Thompson et al. (2017). Security *intention* was adapted from Ifinedo (2012) and Ajzen (1991). *Perceived severity, perceived vulnerability* and perceived realism were adapted from Vance et al.

(2012). The measures for employee security *habit* were adapted from Verplanken and Orbell (2003) and Vance et al. (2012). *Hardiness* scales had measures adapted from the Bartone (1991) study. The measures of *stress* were adapted from Ayyagari et al. (2011), Maier et al. (2015) and Moore (2000). The measures for security *behaviour* were adapted from Thompson et al. (2017). (see Appendix A for the full measurement items).

The *hardiness* scale used in this study consisted of 30 items, with ten items each measuring *commitment, control* and *challenge* dimensions. Consistent with previous studies on hardiness (Kobasa, 1979; Bartone et al., 1989), all three dimensions were measured separately. Hardiness was conceptualised as a second-order construct consisting of its three dimensions as a first-order sub-construct. All measures including hardiness sub-constructs were reviewed according to Jarvis et al. (2003) and MacKenzie et al. (2011) recommendations. All first-order constructs were measured reflectively. *Hardiness* as a second-order construct was measured as a formative construct (that is reflective first-order, formative second-order construct).

4.3.3 Scenario design

The survey was designed to capture SME employees' behavioural intention towards information security when working from multiple locations using BYOD. The hypothetical work scenario was used to measure the threat appraisal of the respondents (*perceived vulnerability* and *perceived severity*) and their *intention* to act like the scenario character in the scenario.

Prior information systems studies have used scenarios (D'Arcy and Hovav, 2009; Guo et al., 2011; Vance et al., 2012; Johnston et al., 2016). There are three key advantages of using scenario-based methods. Firstly, scenario methods are commonly used to assess antisocial and ethical/unethical behaviour (Pogarsky, 2004). Secondly, a hypothetical scenario allows participants to respond honestly because they feel less intimidated to observe and self-report the likelihood of committing the act described in the scenario (Siponen and Vance, 2010; Willison et al., 2016). Thirdly, using scenario methods can improve internal validity of the study (Cheng et al., 2013).

The study used four hypothetical scenarios to capture responses on security behaviours when working from multiple locations. Each scenario was randomly presented to the participants when completing the survey. The four scenarios presented to the respondents had similar criteria such as a work task to be performed using a personal device with the task requiring access to sensitive information. The other criteria which made each scenario different were: location, amount of urgency for the task and type of Wi-Fi connection (see Appendix A).

The scenarios were developed based on the literature and industry security reports, highlighting information security risk accompanying employee use of BYOD and anywhere working trends especially among SMEs (Cisco, 2017; Telstra, 2018). A single measurement item, perceived realism, adapted from Vance et al. (2012) was used to assess the reality of the scenario presented to the respondents. This was suitable for this study, and although a single item measure cannot be validated, Straub et al. (2004) noted that in some situations a single measure is appropriate.

4.3.4 Ethical considerations

A research project involving the collection of data from human subjects either through surveys, interviews, or focus groups requires ethics approval. The National Statement on Ethical Conduct in Human Research outlines research guidelines that researchers must adhere to when conducting research involving human subjects (NHMRC, 2015). The research project and details were submitted to the University's Human Research Ethics Committee (HREC). The ethics committee granted approval to conduct the research before data collection (see Appendix B).

4.3.5 Survey pretest and refinement

A preliminary draft of the full survey was pretested on a group of 15 postgraduate students within the university and six information systems researchers (in Australia, Canada and Germany). The pretest objective was to test scenarios to ascertain if they were relevant, realistic, and understandable (Siponen and Vance, 2014). A pretest is a preliminary trial of the research instrument to ensure that there are no anticipated difficulties (Boudreau et al., 2001). Straub (1989) suggested that content validity of an instrument is established through literature reviews and pretesting the research instrument. The feedback from the pre-testers provided some suggestions for adjusting the scenarios instructions to avoid any ambiguities when presented to the participants. The survey was refined based on feedback from the pretest, and the measurement items were checked for correct grammar, wording and for the completion time of the survey. The final survey was designed, tested and hosted on the University's Qualtrics website to generate a URL link for the distribution of the survey through MTurk.

4.4 Data collection

There were several options available for data collection. The first option was to use a large organisation's SMEs client's database. However, due to factors outside the researcher's control, data collection was not possible using this database.

The second option was to work with a university research librarian to use an online database to access SMEs. However, due to privacy concerns, only business names were listed on the database making it problematic to contact the SMEs directly. To obtain a detailed list of SMEs contact from the business database required an access fee which the research project could not afford.

The final option was to recruit respondents from online platforms for data collection. Amazon Mechanical Turk was selected as the source for data collection based on recommendations from Lowry et al. (2016) and its recent usage in information systems including security studies such as (Tsai et al., 2016; D'Arcy and Lowry, 2017; Menard et al., 2017).

4.4.1 Amazon Mechanical Turk (MTurk)

The primary data collection for the study was obtained from Amazon Mechanical Turk (MTurk). MTurk offers individuals (called requesters) looking to complete tasks referred to as human intelligence task (HIT), a diverse population of individuals (called workers) from different countries willing to carry out the tasks. Studies on the demographic characteristics of MTurk claim that there are more than 500,000 users from over 190 countries with the US having the highest number of users (Chandler and Shapiro, 2016; D'Arcy and Lowry, 2017). Requesters have to pay workers recruited to complete a HIT, Lowry et al. (2016) suggest that researchers offer a reasonable level of pay equivalent to federal minimum wage suitable for HIT advertised.

MTurk offers behavioural study researcher access to high data quality that is similar to data collected from other traditional sources such as laboratories or non-internet samples (Crump et al., 2013). The literature on the use of MTurk shows that workers are afforded more anonymity allowing them to respond honestly to the study requirements with less coercion than traditional methods of data collection (Chandler and Shapiro, 2016). Another study found that MTurk data obtained by researchers met acceptable psychometric properties, especially when restricted to the U.S. only samples (Steelman et al., 2014). Additionally, Lowry et al. (2016) study offer researchers guidelines to overcome the hurdles and limitations on MTurk to ensure data quality when obtaining data from workers and reporting results.

4.4.2 Recruitment of MTurk workers

Requesters on MTurk have to advertise their tasks (HIT) stating the criteria that should be met before accepting a task and the amount a worker receives upon completion of a HIT. Using guidelines from Lowry et al. (2016), the survey prepared on Qualtrics was advertised on MTurk where workers who met the required criteria for the study were recruited. Detailed instructions were included because this has been shown to increase the quality of data when using MTurk (Crump et al., 2013) (see Appendix C).

MTurk provides automatic filters called qualification to restrict HIT to certain workers. The HIT was available only to workers who reside in the U.S. and workers who responded to the survey were excluded from participating from subsequent reposting of the HIT to ensure that each response was unique. The study advertisement was entitled 'A survey about using a personal device at work.' The title was vague so as not to alert workers previewing the HIT advertisement on the information security behaviour context and submit dishonest responses to the survey questions (Chandler and Shapiro, 2016). The Qualtrics survey link was included in the MTurk HIT enabling workers who accepted the HIT to proceed and submit their response.

A 2.00 USD fee was paid to 294 respondents for completing the survey. MTurk allows requesters to deny payment to workers who submit responses that do not meet acceptable data quality (Steelman et al., 2014). The detail of the data screening is explained in the data analysis section.

4.4.3 Pilot testing

On MTurk a pilot test was conducted after the pre-test (Straub, 1989). An initial project was created on MTurk website advertising for 30 responses. The responses were filled quickly (less than ten hours). On MTurk, the data file containing the worker's details and the unique code was export, and the data file on Qualtrics was also exported. Following the pilot testing, the average completion time was checked, the arrangement of the survey questions and attention filters was refined for the final data collection. The quick response on MTurk encourages pilot tests, data collection is fast and can be conducted at any time regardless of the respondent's location (Lowry et al., 2016).

4.5 Data analysis procedure

A total of 382 participants were recruited through MTurk. However, not all responses submitted were usable. This section provides details of the data screening, validation, reliability and analysis.

4.5.1 Data screening

After the pre-test and pilot, the HIT was posted on the MTurk site to collect the data. The HIT was reposted after screening and excluding invalid data from the responses collected. An attention filter question was embedded among the measurement items (for example "Where is the statue of liberty located") to ensure respondents paid attention to the question and answers they provided. Respondents who failed the attention filter question were excluded from the data analysis. Responses exhibiting certain patterns, such as selecting 4’s only or alternating 6 and 7 were removed from the data analysis. Participants who completed the survey in an unreasonably short time (below five minutes) were also excluded from the data.

An IP address check was carried out to ensure all responses submitted were from the U.S. First, an email was sent to MTurk to clarify the effectiveness of the workers location exclusion criteria. MTurk claimed that a worker's location is provided at the time of registering their account and is tied to their account. Second, a third party website[1] was used to check all IP addresses captured in the survey data to ensure they were U.S. based.

4.5.2 Data validation and reliability

Psychometric tests were conducted on the data to determine if the measures in the survey were reliable to produce valid results (Recker, 2013). A validity test checks whether the measures chosen by the researcher are what it claims to be measuring, that is, if the measures are true constructs describing the event or merely artefacts of the methodology (Straub, 1989; Straub et al., 2004). There are two statistical techniques recommended in the literature to test the validity of the data collected: convergent validity and discriminant validity.

Convergent validity is when items thought to reflect a construct converge, or show significantly high correlations with one another (Straub et al., 2004). Discriminant validity is present when construct items do not differ from other construct items, especially where the items are unrelated (Straub, 1989). Hair et al. (2011) recommended that to establish convergent validity, construct should have an average variance extracted (AVE) of 0.50 or higher. According to Hair et al. (2011) the Fornell-Larcker criterion should be used to evaluate the discriminant validity; the AVE of each construct should be higher than the construct’s highest squared correlation with any other construct. More recently Hair et al. (2017) suggested that the heterotrait-monotrait ratio (HTMT) should be assessed for values lower than 0.90 to establish discriminant validity.

Reliability of the data refers to an evaluation of measurement accuracy, that is the extent to which the respondent answered the same or approximately the same questions the same way each time (Straub, 1989). Composite reliability values are used to assess the reliability of the data, values of 0.60 to 0.70 is considered acceptable (Hair et al., 2011, 2017). The purpose of

---

[1] https://www.infobyip.com/

validating and ensuring the reliability of data using statistical tests is to substantiate the results and findings of the data collected (Straub, 1989; Boudreau et al., 2001).

4.5.3 Data analysis

There were 294 final usable responses. Structural equation modelling (SEM) techniques were used to test the theoretical model. SEM is more suited for multidimensional models and provides the flexibility to model relationships among multiple predictors and criterion variables, construct unobservable latent variables, and statistically test theories (Chin, 1998; MacKenzie et al., 2005).

SmartPLS was used to analyse the theoretical model. SmartPLS was chosen over covariance-based SEM (CB-SEM) technique such as LISREL or AMOS because the theoretical model in the study was for predictive purposes rather than just theory testing. (Chin, 1998; Siponen and Vance, 2010). SmartPLS maximises the explained variance of the endogenous (latent) construct and offers higher levels of statistical power when testing theories (Hair et al., 2011, 2014b). Prior behavioural information security studies used SmartPLS when testing the research model (Siponen and Vance, 2010; Ifinedo, 2012; Johnston et al., 2015; D'Arcy and Lowry, 2017). The next chapter presents an in-depth analysis of the data analysis and results using SmartPLS 3.2.7.

4.6 Summary

In this chapter, an overview of the research method and data collection procedure were presented. A quantitative survey was designed, participants for data collection were recruited from Amazon MTurk. Several screening processes according to the literature were used to ensure the quality of the data collected. The next chapter presents and discusses the results of the data analysis.

Chapter 5: Data Analysis and Results

5.1 Introduction

This chapter presents the assessments of the measurement model using the following tests: common method bias, content validity, construct reliability and validity. After all criteria met the required threshold and cut-offs, assessment of the structural model was conducted using a bootstrapping technique to test for significant paths coefficient, effect sizes and total variance of the model. Finally, the results of the data analysis are presented

The next sections presents the analysis and results of the data collected to answer the research question. Partial least squares (PLS) is a structural equation modelling (SEM) technique which uses a component-based estimation (Ifinedo, 2014). PLS is useful for models that have higher-order constructs (second-order construct) and more suitable for prediction purposes than theory testing (Lowry and Gaskin, 2014). SmartPLS 3.2.7 (Ringle et al., 2015) was the specific SEM software used to analyse the theoretical model.

5.2 Data analysis

Table 3 shows the descriptive statistics of the study. Both male and female are almost equally distributed (54 vs. 46), and more than half (52.4%) of the sample is between the ages of 25 and 34 years and 50% of the respondents completed a Bachelor’s degree. Only 4.8% of the respondents are business owners, 49% of the respondents combined work as technical and managerial personnel, and 31% work in professional, scientific and technical services industries. More than half of the respondents work in medium-sized organisations. Over 75% of the respondents had worked with their organisation for over four years. A large number of the respondents, 79% claim to have an ISP and are aware of the policy content (mean=2.13, SD=1.73), in the organisation while only 64% have a BYOD policy they (mean=1.63, SD=1.67). From the analysis of ISP availability, medium-sized organisations tended to have security policies (81.3% vs 18.7%) and a BYOD policy (72.5% vs 27.5%) more than small businesses.

Table 3: Demographic statistics of the study

		frequency	**percent**
Gender	Male	159	54.08%
	Female	135	45.92%
Age range	18 - 24	29	9.86%
	25 - 34	154	52.38%
	35 - 44	78	26.53%
	45 - 54	22	7.48%
	55 and above	11	3.74%
Education	High school	30	10.20%
	Vocational training	14	4.76%
	Diploma (Advance diploma, Associate degree)	47	15.99%
	Bachelor’s degree	144	48.98%
	Master’s degree	48	16.33%
	Doctorate	7	2.38%
	Other	4	1.36%
Organisational role	Owner	14	4.76%
	Administrative	55	18.71%
	Technical	69	23.47%
	Managerial	75	25.51%
	Supervisory	39	13.27%
	Consultant	34	11.56%
	Other	8	2.72%
Industry	Manufacturing	29	9.86%
	Construction	8	2.72%
	Finance and Insurance services	32	10.88%
	Accommodation and food services	13	4.42%
	Professional, Scientific and Technical services	92	31.29%
	Rental, Hiring and Real Estate Services	14	4.76%
	Health care and Social Assistance	40	13.61%
	Education and Training	42	14.29%
	Other	24	8.16%
Organisational size	0 - 4	16	5.44%
	5 - 19	59	20.07%
	20 - 199	125	42.52%
	200 - 499	67	22.79%
	500 - 999	27	9.18%
Organisational tenure	0 - 4	141	47.96%
	5 - 9	117	39.80%
	10 - 14	24	8.16%
	more than 15 years	12	4.08%
Availability of information security policy	Yes	235	79.93%
	No	27	9.18%
	I don't know	32	10.88%
Availability of BYOD policy	Yes	190	64.63%
	No	54	18.37%
	I don't know	50	17.01%

5.2.1 Common method bias

Before evaluating the model, the common method variance test was conducted to test whether common method bias was a concern. Common method bias (CMB) in behavioural research threatens the validity of statistical results drawn. CMB occurs in self-reported studies when measures of the dependent and independent variables are taken from the same source (Podsakoff et al., 2003). There are two main methods used to assess and minimise CMB:

procedural and statistical remedies. Procedural remedies for controlling for CMB were followed to minimise bias when respondents received the questionnaire (Podsakoff et al., 2012). The procedures were clear and concise questions were used in the survey instrument, and participants were assured of anonymity to reduce apprehension.

Before evaluating the structural model, the statistical remedy (Harman's single-factor test) was used to assess whether CMB was an issue in the sample data. Podsakoff et al. (2003) recommended behavioural researchers check for CMB using Harman's single-factor test to see if one factor accounted for the majority of variance in the data. All items in the survey instrument were entered into an unrotated factor analysis. Results from the test showed that the largest factor accounted for 26 per cent of the variance showing that CMB was not an issue with the data. Additionally, the latent construct correlation was examined, no two-latent construct correlated highly at .90 or more (Vance et al., 2012).

5.2.2 Assessment of the measurement model

Following the procedures outlined in Lowry and Gaskin (2014), the model assessment was carried out. First, content validity was established through the use of well-established theories and adaptation of constructs from previously validated studies (Straub et al., 2004). Next, convergent validity was evaluated by the item loadings and the average variance extracted (AVE). Gefen and Straub (2005) and Hair et al. (2017) recommend that item loadings should be above the 0.60 cut-offs and the AVE of all constructs should be above the 0.50 threshold. Table 4 shows all items of the theoretical model significant above the 0.60 cut-offs, items which loaded poorly were dropped from further observation. The AVE of all constructs was greater than the threshold value of 0.50 (Table 4). The construct reliability was evaluated by composite reliability where values should be higher than 0.70 (Chin, 1998; Hair et al., 2011). Table 4 shows the composite reliability and Cronbach's Alphas values of all constructs were adequately above 0.70 thresholds.

Table 4: Descriptive statistics of constructs, loadings, significance, AVE, and reliability statistics

Construct	**Items**	**Mean**	**SD**	**Loadings**	**t-statistics**	**AVE**	**CR**	**CA**
Hardiness commitment	HARDCM1	5.350	1.240	0.810	31.851	0.668	0.909	0.876
	HARDCM3	5.390	1.350	0.827	33.477			
	HARDCM4	5.160	1.410	0.822	37.944			
	HARDCM6	5.620	1.130	0.793	34.671			
	HARDCM8	5.030	1.480	0.834	41.579			
Hardiness control	HARDCO14	5.450	1.190	0.752	20.361	0.534	0.820	0.709
	HARDCO15	5.570	1.130	0.696	13.963			
	HARDCO16	5.360	1.240	0.770	27.695			
	HARDCO20	5.390	1.180	0.702	15.661			
Hardiness challenge	HARDCH23	5.640	1.120	0.773	27.151	0.528	0.817	0.707
	HARDCH25	5.380	1.300	0.692	15.420			
	HARDCH27	4.900	1.420	0.746	26.024			
	HARDCH30	4.470	1.510	0.692	16.174			
Stress	STRESS1	2.490	1.730	0.911	43.722	0.787	0.937	0.910
	STRESS2	3.050	1.780	0.815	30.091			
	STRESS3	2.310	1.720	0.910	61.453			
	STRESS6	2.410	1.620	0.910	62.098			
Attitude	ATTITUDE1	6.030	1.160	0.864	44.907	0.744	0.936	0.914
	ATTITUDE2	6.190	1.090	0.886	58.754			
	ATTITUDE3	5.960	1.190	0.870	45.736			
	ATTITUDE4	6.160	1.110	0.881	39.615			
	ATTITUDE5	6.170	1.030	0.809	27.818			
Perceived severity	SEVERITY1	5.980	1.210	0.944	87.106	0.762	0.864	0.710
	SEVERITY2	5.420	1.510	0.795	17.282			
Perceived vulnerability	VULN1	5.720	1.420	0.817	17.447	0.794	0.920	0.869
	VULN2	5.790	1.420	0.934	81.503			
	VULN3	5.840	1.370	0.918	56.558			
Subjective norms	SNORM1	5.150	1.700	0.939	63.895	0.876	0.955	0.930
	SNORM2	5.280	1.680	0.941	89.945			
	SNORM3	5.370	1.610	0.928	70.429			
Habit	HABIT1	5.870	1.130	0.795	29.955	0.633	0.939	0.927
	HABIT10	5.630	1.340	0.755	20.034			
	HABIT11	5.310	1.440	0.723	17.739			
	HABIT12	5.360	1.500	0.670	12.978			
	HABIT3	5.710	1.310	0.848	45.114			
	HABIT4	5.850	1.280	0.834	38.554			
	HABIT5	5.760	1.310	0.880	59.907			
	HABIT6	5.550	1.380	0.831	35.054			
	HABIT8	5.590	1.330	0.802	25.371			
Intention	INT1	6.220	1.040	0.949	111.110	0.881	0.957	0.932
	INT2	6.210	1.030	0.943	105.169			
	INT3	6.290	0.970	0.924	81.781			
Behaviour	BEH1	5.850	1.560	0.945	82.991	0.873	0.932	0.855
	BEH4	5.970	1.510	0.923	41.956			

Legend: AVE = Average Variance Extracted; CR = Composite Reliability; CA = Cronbach’s Alpha; all t-statistics significant at p<.01

The assessment of discriminant validity was evaluated using two measures, the Fornell-Larcker criterion and the cross loadings of each construct (Hair et al., 2011). Hair et al. (2017) recent update on the assessment of discriminant validity, recommends the heterotrait-monotrait ratio

(HTMT) criterion when reporting discriminant validity. The Fornell–Larcker criterion recommends that the square root of the AVE of each construct should be larger than the inter-construct correlations (Hair et al., 2011; D'Arcy et al., 2014b). The Fornell–Larcker values are shown in Table 5, all constructs loaded highly on their corresponding construct. The HTMT ratio of correlations recommends that the indicators of any two constructs should exhibit values that are smaller than one to establish discriminant validity (Henseler et al., 2015). The items in Table 6 with HTMT values above 0.85 have questions that are similarly worded in the survey. However, discriminant validity is established between the constructs because the HTMT values shown in Table 6 have values lower than the 0.90 threshold (Hair et al., 2017). All items loadings in Table 7 loaded strongly on their respective construct when compared to the loadings of other items against other constructs (Hair et al., 2011; MacKenzie et al., 2011).

Table 5: Discriminant validity – the Fornell-Larcker criterion

Item	**Att**	**Bh**	**Habit**	**HardCH**	**HardCM**	**HardCO**	**Int**	**Psev**	**Pvul**	**Snorm**	**Stress**
Att	0.863										
Bh	0.521	0.934									
Habit	0.769	0.464	0.795								
HardCH	0.371	0.242	0.384	0.726							
HardCM	0.353	0.222	0.303	0.671	0.817						
HardCO	0.531	0.340	0.502	0.618	0.701	0.731					
Int	0.816	0.459	0.762	0.343	0.322	0.491	0.939				
Psev	0.537	0.287	0.468	0.236	0.219	0.333	0.504	0.873			
Pvul	0.385	0.196	0.356	0.211	0.183	0.288	0.355	0.505	0.891		
Snorm	0.286	0.301	0.285	0.189	0.210	0.283	0.319	0.201	0.222	0.936	
Stress	-0.435	-0.218	-0.406	-0.078	-0.145	-0.235	-0.446	-0.252	-0.193	-0.069	0.887

Legend: Att = Attitude; Bh = Behaviour; Int = Intention; HardCH = Hardiness Challenge; HardCM = Hardiness Commitment; HardCO = Hardiness Control; Psev = Perceived Severity; Snorms = Subjective Norms; Pvul = Perceived Vulnerability

Table 6: Discriminant validity - Heterotrait-Monotrait Ratio (HTMT)

Item	**Att**	**Bh**	**Habit**	**HardCH**	**HardCM**	**HardCO**	**Int**	**Psev**	**Pvul**	**Snorm**	**Stress**
Att											
Bh	0.588										
Habit	0.827	0.502									
HardCH	0.437	0.284	0.455								
HardCM	0.396	0.258	0.335	0.820							
HardCO	0.664	0.442	0.616	0.840	0.884						
Int	0.883	0.511	0.810	0.406	0.357	0.607					
Psev	0.629	0.336	0.539	0.312	0.271	0.466	0.576				
Pvul	0.432	0.230	0.389	0.254	0.211	0.375	0.393	0.690			
Snorm	0.311	0.334	0.302	0.211	0.234	0.359	0.340	0.234	0.246		
Stress	0.468	0.237	0.434	0.162	0.165	0.292	0.473	0.263	0.210	0.073	

Legend: Att = Attitude; Bh = Behaviour; Int = Intention; HardCH = Hardiness Challenge; HardCM = Hardiness Commitment; HardCO = Hardiness Control; Psev = Perceived Severity; Snorms = Subjective Norms; Pvul = Perceived Vulnerability

A multicollinearity assessment was conducted to ensure that two or more constructs did not correlate highly. Collinearity issues arise when high correlations exist between two formative constructs, while multicollinearity is a situation involving more than two constructs (Hair et al., 2014). SmartPLS 3 tests for multicollinearity in the inner and outer model automatically. Multicollinearity is measured by the variance inflation factor (VIF), where values are above ten multicollinearity poses a problem. All first-order constructs in the model were reflective, but the inner and outer VIF values were less than five as recommended in the literature (Hair et al., 2014; 2017). Multicollinearity was not an issue with the study’s results.

Table 7: Indicator item cross loadings

Item	Att	Beh	Int	Habit	HardCH	HardCM	HardCO	Psev	Stress	Snorm	Pvul
ATTITUDE1	**0.864**	0.468	0.700	0.670	0.311	0.328	0.448	0.495	-0.344	0.256	0.367
ATTITUDE2	**0.886**	0.496	0.711	0.672	0.312	0.257	0.423	0.467	-0.421	0.249	0.362
ATTITUDE3	**0.870**	0.388	0.658	0.626	0.341	0.340	0.473	0.412	-0.353	0.251	0.340
ATTITUDE4	**0.881**	0.482	0.714	0.665	0.300	0.281	0.468	0.458	-0.411	0.254	0.326
ATTITUDE5	**0.809**	0.410	0.729	0.682	0.337	0.319	0.478	0.480	-0.343	0.224	0.268
BEH1	0.496	**0.945**	0.459	0.484	0.226	0.206	0.312	0.274	-0.218	0.299	0.206
BEH4	0.476	**0.923**	0.393	0.374	0.227	0.210	0.325	0.262	-0.188	0.260	0.157
INT1	0.762	0.421	**0.949**	0.712	0.308	0.313	0.464	0.454	-0.460	0.288	0.330
INT2	0.766	0.444	**0.943**	0.714	0.320	0.324	0.474	0.481	-0.420	0.296	0.347
INT3	0.768	0.427	**0.924**	0.719	0.337	0.270	0.443	0.483	-0.375	0.314	0.323
HABIT1	0.694	0.467	0.688	**0.795**	0.320	0.305	0.454	0.418	-0.353	0.240	0.326
HABIT10	0.695	0.426	0.613	**0.755**	0.325	0.243	0.455	0.413	-0.313	0.269	0.284
HABIT11	0.487	0.194	0.474	**0.723**	0.285	0.203	0.301	0.279	-0.211	0.155	0.181
HABIT12	0.464	0.240	0.448	**0.670**	0.306	0.222	0.325	0.272	-0.251	0.193	0.207
HABIT3	0.669	0.454	0.660	**0.848**	0.331	0.238	0.409	0.427	-0.323	0.287	0.325
HABIT4	0.651	0.464	0.688	**0.834**	0.274	0.266	0.422	0.421	-0.362	0.243	0.341
HABIT5	0.652	0.374	0.665	**0.880**	0.323	0.239	0.401	0.403	-0.328	0.255	0.288
HABIT6	0.560	0.326	0.592	**0.831**	0.284	0.216	0.386	0.302	-0.351	0.201	0.273
HABIT8	0.573	0.281	0.552	**0.802**	0.315	0.224	0.410	0.363	-0.388	0.168	0.279
HARDCH23	0.388	0.226	0.384	0.353	**0.773**	0.531	0.539	0.290	-0.180	0.181	0.225
HARDCH25	0.229	0.077	0.198	0.190	**0.692**	0.376	0.397	0.035	-0.067	0.063	0.136
HARDCH27	0.303	0.282	0.228	0.346	**0.746**	0.635	0.509	0.234	-0.025	0.229	0.170
HARDCH30	0.103	0.060	0.151	0.181	**0.692**	0.342	0.301	0.062	0.085	0.023	0.047
HARDCM1	0.218	0.154	0.198	0.215	0.554	**0.810**	0.594	0.155	-0.075	0.164	0.062
HARDCM3	0.333	0.195	0.312	0.283	0.503	**0.827**	0.612	0.181	-0.160	0.138	0.181
HARDCM4	0.264	0.160	0.227	0.213	0.547	**0.822**	0.548	0.166	-0.077	0.217	0.126
HARDCM6	0.369	0.223	0.337	0.292	0.503	**0.793**	0.568	0.213	-0.207	0.134	0.250
HARDCM8	0.262	0.179	0.246	0.236	0.633	**0.834**	0.541	0.181	-0.076	0.204	0.132
HARDCO14	0.326	0.249	0.337	0.302	0.437	0.534	**0.752**	0.220	-0.127	0.134	0.184
HARDCO15	0.477	0.321	0.434	0.456	0.391	0.429	**0.696**	0.353	-0.266	0.244	0.295
HARDCO16	0.418	0.233	0.364	0.436	0.518	0.584	**0.770**	0.213	-0.189	0.131	0.174
HARDCO20	0.340	0.199	0.307	0.276	0.451	0.487	**0.702**	0.202	-0.111	0.340	0.204
SEVERITY1	0.556	0.316	0.535	0.481	0.206	0.213	0.321	**0.944**	-0.295	0.207	0.380
SEVERITY2	0.336	0.145	0.290	0.298	0.218	0.163	0.252	**0.795**	-0.093	0.129	0.578
STRESS1	-0.383	-0.174	-0.349	-0.344	-0.089	-0.157	-0.246	-0.229	**0.911**	-0.058	-0.167
STRESS2	-0.284	-0.102	-0.279	-0.292	-0.057	-0.127	-0.156	-0.107	**0.815**	-0.006	-0.091
STRESS3	-0.426	-0.256	-0.432	-0.356	-0.018	-0.075	-0.177	-0.237	**0.910**	-0.059	-0.199
STRESS6	-0.424	-0.214	-0.487	-0.433	-0.111	-0.161	-0.244	-0.287	**0.910**	-0.105	-0.204
SNORM1	0.260	0.287	0.324	0.265	0.150	0.191	0.247	0.195	-0.056	**0.939**	0.198
SNORM2	0.276	0.298	0.305	0.286	0.203	0.191	0.275	0.192	-0.085	**0.941**	0.205
SNORM3	0.268	0.255	0.259	0.248	0.181	0.211	0.277	0.177	-0.052	**0.928**	0.223
VULN1	0.315	0.225	0.280	0.276	0.179	0.158	0.249	0.379	-0.158	0.157	**0.817**
VULN2	0.345	0.144	0.325	0.314	0.204	0.183	0.273	0.481	-0.204	0.204	**0.934**
VULN3	0.368	0.165	0.341	0.357	0.181	0.148	0.250	0.481	-0.155	0.227	**0.918**

Legend: Att = Attitude; Bh = Behaviour; Int = Intention; HardCH = Hardiness Challenge; HardCM = Hardiness Commitment; HardCO = Hardiness Control; Psev = Perceived Severity; Snorms = Subjective Norms; Pvul = Perceived Vulnerability

5.2.3 Assessment of the structural model

In testing the theoretical model, the effect of the control variables was evaluated: age, gender, years of work, organisational size and perceived realism of the scenario. To evaluate the control variables, dummy variables were created following Henseler et al. (2017) and included in the exogenous variables to assess for effect on the dependent variable. The perceived realism of the scenario that was randomly assigned to each participant was also evaluated. As shown in Table 8, the control variables did not significantly influence security behaviours of the respondents (r^2=0.255, control variables included).

Table 8: Control variables result

Effect	**estimate**	**SD**	**t-value**
Gender	0.078	0.050	1.566
Age	0.066	0.091	0.730
Years of Work	0.081	0.118	0.691
Organisational Size	0.130	0.104	1.259
Perceived Realism	0.065	0.044	1.496

The structural model shows information about the significant path coefficients (Figure 4). In PLS, the bootstrapping method is used to test the significance of paths and R squared (R^2). In this study to test the significant path coefficients and r^2, 5000 bootstrap samples were used (Hair et al., 2017). Chin (1998) suggests that high r^2 values demonstrate the predictive power of the PLS model, where r^2 values of 0.67, 0.33 and 0.19 are substantial, moderate and weak respectively. The results of the bootstrap are summarised in Table 9 and Figure 4 shows the results of the structural model. The model explains a considerable amount of variance in security intentions, that is 71%, but only 21% of the variance in security behaviours. The r^2 values of the structural model are substantial with intention at 0.717 and behaviour moderate at 0.210.

Table 9: Effect sizes, t-statistics and confidence intervals

Path	**Std Beta(β)**	**Std Error**	**t-value**	**Effect (f^2)**	**2.5%CI**	**97.5%CI**
Attitude -> Intention	0.524	0.072	7.255***	0.352	0.371	0.658
Habit -> Intention	0.311	0.06	5.201***	0.136	0.201	0.434
Hardiness -> Attitude	0.401	0.051	7.798***	0.238	0.296	0.499
Intention -> Behaviour	0.450	0.057	7.831***	0.251	0.341	0.564
PSeverity -> Intention	0.066	0.049	1.363+	0.009	-0.029	0.162
PVulnerability -> Intention	-0.006	0.042	0.144+	0.000	-0.085	0.079
SNorms -> Intention	0.068	0.031	2.224*	0.015	0.008	0.127
Stress -> Attitude	-0.364	0.049	7.464***	0.196	-0.462	-0.271

*p<0.05, **p<0.01, ***p<0.001, + = not significant (p>0.05)
Effect sizes: 0.02 small, 0.15 medium, 0.35 large (Cohen, 1988)

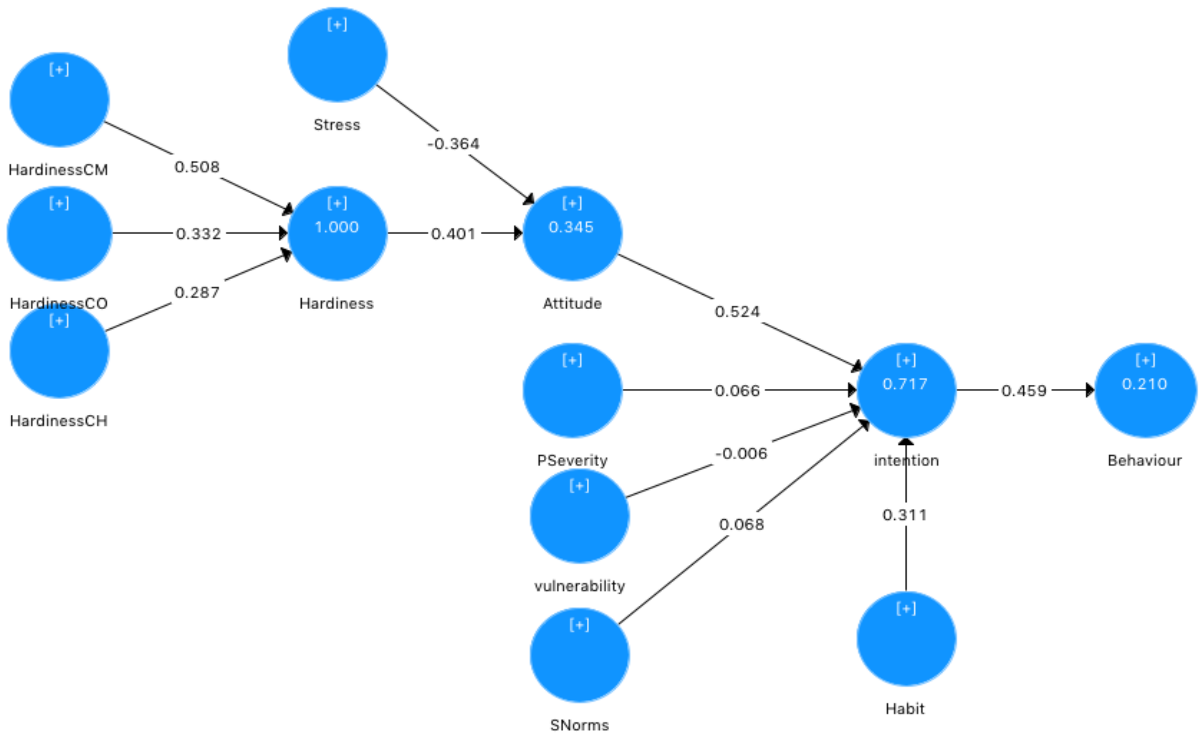


Figure 4: Result of the structural model

Additionally, the structural model path coefficients effect sizes (f^2) were evaluated (Hair et al., 2012). Cohen (1988) suggests that f^2 values of 0.02, 0.15, and 0.35 indicates small, medium and large effects respectively. Table 9 shows that perceived severity and vulnerability have no effect on intention, while the remaining constructs have different effect sizes.

To assess the predictive relevance (q^2) of the model, the Stone-Geisser test was conducted, in SmartPLS blindfolding, using an omission distance of 8 (Hair et al., 2017). The resulting q^2 values of larger than 0 indicate that the model constructs have predictive relevance and values less than 0 indicate a lack of predictive relevance (Hair et al., 2012). Results shown in Table 10 show that the model has good predictive relevance.

The goodness-of-fit (GoF) refers to the extent to which all constructs and relationships within a model can be reproduced (Hair et al., 2017). In evaluating the GoF for the model, Henseler and Sarstedt (2013) recommend a careful evaluation of the path coefficients and particularly their significance to decide which paths to leave in the model and which to discard. Moreover, the theoretical model consists of higher-order constructs (hardiness as a second-order construct), GoF is conceptually inappropriate when the outer model is formative (Hair et al., 2012). Overall, the assessment (r^2, f^2, q^2, β, and t-values) shows that the study's theoretical model is structurally sound and possesses adequate predictive relevance.

Table 10: r squared and q squared values

	r^2	q^2
Attitude	0.345	0.242
Behaviour	0.210	0.175
Hardiness	1*	0.434
Intention	0.717	0.599

* Formative construct

R Squared: 0.67- substantial, 0.33- moderate, 0.19- weak (Chin, 1998)

Q Squared: 0.02- weak, 0.15- moderate, 0.35- strong. Stone–Geisser's q2 (Hair et al., 2014)

5.3 Results of the theoretical model analysis

The aim of the study was to investigate the factors that employees perceive may change security behaviour when performing work tasks using BYOD from multiple locations. Contrary to expectations of the theoretical model (Figure 4), the threat appraisal had an insignificant effect on security *intentions*; *perceived severity* (β 0.066) and *perceived vulnerability* in the opposite direction was not expected (β -0.006). The role of social influences, *subjective norms* (β 0.068; $p<0.05$), did not have a strong influence on security *intention*.

The *stress* of dealing with information security requirements had a significant effect on *attitude* (β-0.364; $p<0.001$). The *hardiness* personality traits had a stronger effect on *attitude* (β0.401; $p<0.001$) than the *stress* of security requirements. *Attitude* had *stress* and *hardiness* as antecedents, with a variance of 34%; *attitude* had a significant influence on security *intentions* (β 0.524; $p<0.001$). As expected *habit* had a strong influence on security intentions (β 0.311; $p<0.001$).

5.3.1 Multi-Group analysis

The Multi-Group analysis (MGA) was conducted to test for differences between path coefficients based on the scenario the respondent randomly received. MGA is a technique in SmartPLS used to test the means of predefined groups to determine if there are significant differences between group-specific parameter estimates (Hair et al., 2014). The results in Table 11 shows that the scenario received did not have any effect on the security intentions of the respondents. Table 12 shows the AVE of both constructs in the MGA, all above the 0.50 cut-off.

Table 11: MGA: Welch-Satterthwaite test

Path		scene1-scene2	scene1-scene3	scene1-scene4	scene2-scene3	scene2-scene4	scene3-scene4
Attitude -> intention	Path Coefficients	0.101	0.069	0.200	0.033	0.099	0.131
	t-value	0.509	0.296	0.921	0.168	0.557	0.616
	p-value	0.612	0.768	0.360	0.867	0.579	0.540
SNorms -> intention	Path Coefficients	0.013	0.040	0.032	0.028	0.019	0.008
	t-value	0.151	0.409	0.375	0.312	0.263	0.094
	p-value	0.880	0.684	0.709	0.756	0.793	0.925
Hardiness_ -> Attitude	Path Coefficients	0.108	0.138	0.380	0.030	0.272	0.242
	t-value	0.746	1.157	2.492	0.222	1.633	1.659
	p-value	0.458	0.251	0.015	0.825	0.107	0.102
Stress -> Attitude	Path Coefficients	0.049	0.130	0.207	0.081	0.158	0.076
	t-value	0.380	1.235	1.861	0.568	1.069	0.596
	p-value	0.705	0.221	0.067	0.572	0.289	0.553
Habit -> intention	Path Coefficients	0.060	0.037	0.132	0.097	0.072	0.169
	t-value	0.366	0.184	0.700	0.569	0.453	0.871
	p-value	0.716	0.854	0.487	0.571	0.652	0.387
PSeverity -> intention	Path Coefficients	0.205	0.112	0.008	0.093	0.197	0.104
	t-value	1.508	0.888	0.052	0.741	1.218	0.676
	p-value	0.136	0.377	0.959	0.461	0.228	0.501
vulnerability -> intention	Path Coefficients	0.249	0.261	0.042	0.012	0.207	0.220
	t-value	1.925	1.915	0.299	0.102	1.667	1.667
	p-value	0.058	0.059	0.766	0.919	0.100	0.100
intention -> Behaviour	Path Coefficients	0.015	0.053	0.032	0.039	0.047	0.085
	t-value	0.092	0.338	0.224	0.229	0.300	0.553
	p-value	0.927	0.736	0.823	0.820	0.765	0.582

In the MGA, the strength of habit in each scenario on security intention was observed, the effect of habit varied slightly with both locations. When working at the office with BYOD, it can be observed that coefficient paths for office scenarios (scene1 ß=0.348; scene3 ß=0.385) were slightly higher than the café scenarios (scene2 ß=0.288; scene4 ß=0.216). Overall, each construct in MGA of the scenarios, except *habit*, measured close to the general model.

Table 12: AVE of scenarios

	PSeverity	vulnerability
Scene1 (n=75)	0.690	0.787
Scene2 (n=73)	0.791	0.765
Scene3 (n=78)	0.759	0.800
Scene4 (n=68)	0.821	0.785

5.4 Summary

This chapter presented the analysis of the quantitative data collected. Psychometric evaluation of the data showed that the measurement items were reliable and valid, and common method bias was not an issue. Results from the theoretical model show that the threat appraisal process did not influence employee's security *intention*. Social influence from the environment had a small effect and habit had a significant effect on security intention. *Stress* and *hardiness* strongly influence attitude and strengthen security behavioural intentions. The overall analysis of the model showed that behavioural *intention* accounted for 71% of variance while *behaviour* had 21%. The next chapter discusses the results and significant findings.

Chapter 6: Discussion

6.1 Introduction

The discussion presented in this chapter highlights the key findings from the study. The chapter concludes with the study's contribution to theory and practice.

The purpose of this study was to investigate the factors that may change the security behaviours of SME employees when using their devices (BYOD) for work purposes from different work locations. BYOD use by employees when working anywhere is a risk to organisational information. SMEs need to ensure that employees' security behaviours when working from alternative locations using BYOD comply with security policies and minimise threats when accessing organisational data.

6.2 Discussion of key findings

The theoretical model was developed using components from protection motivation theory (PMT), theory of planned behaviour (TPB), habit, hardiness, and stress from the literature on technostress. These theories were selected because the constructs in the theories help us understand employees' cognitive, social and behavioural factors that influence their security behaviours. The model in Figure 5 shows that employees' security behaviours are subject to change because of the strong path from a user's security intention to their security behaviour.

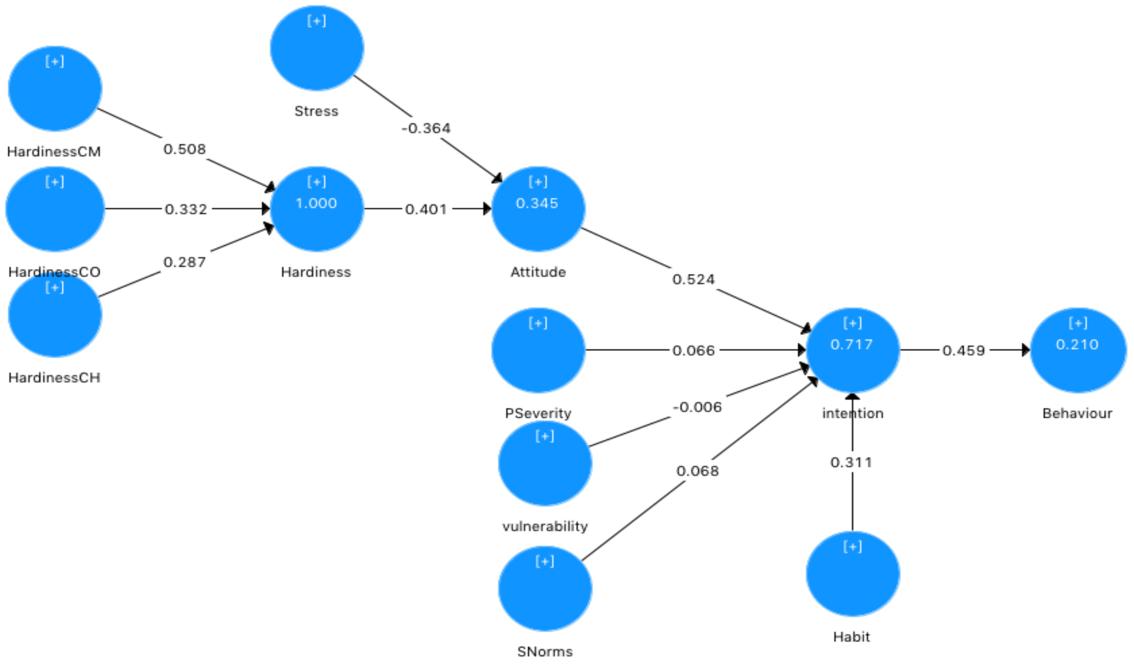


Figure 5: SME employees' security behaviour model

There are three key findings in the study. First, *hardiness*, *stress* and *habit* have a significant effect on an employee's security intention. Second, *hardiness* has a stronger effect on security intentions than *habit* or *stress*. Finally, the threat appraisal (*perceived vulnerability* and *severity*) process does not have any effect on employees' security *intention*.

6.2.1 Hardiness and information security behaviours

In the context of information security, the results showed that *hardiness* personality traits play a key role in determining employees' security behavioural intention. Personality traits frame how individuals perceive security threats. Employees' security behaviours differ when responding to security requirements and threats based on their hardiness levels. The results showed that employees who had high levels of *hardiness* personality traits: *commitment, control* and *challenge*, can overcome security threats by making adjustments where necessary and irrespective of their work location to minimise the effect of security threats rather than avoid or submit to the security threat.

The *commitment* disposition is the most important factor in motivating employees to engage in positive security behaviours because commitment implies a deep connection to the organisation. Posey et al. (2015) asserted that employees who are highly committed to their organisation focus on the protection of information assets and take an interest in information security to benefit the organisation rather than themselves. This study showed that employees who signal a high level of commitment also signal that they would be more adaptable and more likely to harness security resources from work locations such as undertaking appropriate security measures and behaviours to combat information security threats. High levels of commitment to work in employees psychologically prepare them to be more cautious of security threats to their organisation’s information assets arising from different locations of work, causing the employee to take proactive security measures (Bartone, 2006).

The *control* disposition is the second most important factor that influences an employee’s security behaviour. Employees with a high level of control can control work events around them to produce favourable outcomes. Employees use control as a mechanism to mitigate information security-related stress (SRS), relying on their knowledge, a range of skills, abilities and expertise to meet the demands of stressful security procedures. This study confirms prior studies in that if employees have the relevant competence, skill and knowledge to take security precautions, they are more likely to engage in positive security behaviours (Bulgurcu et al., 2010; Ifinedo, 2012). Moreover, the hardiness control disposition enhances employees’ attitudes to comply with security policies and equips them with a resilience attitude in dealing with information security-related stress and threats.

The third most important disposition of the hardiness personality trait was *challenge*. An employee with a high level of the challenge disposition will be capable of handling unexpected security events at work locations when they occur. Employees working in a public location will make a security readjustment from their experience and develop security behaviours to protect their work and organisational information assets. Similarly, challenge buffers the effect of security and work stress that employees may experience. Security requirements may vary at alternative locations of work, however, employees who exhibit a high level of the challenge disposition will perceive the security-related stress as an avenue to learn and increase their security capabilities. Also, these employees learn, grow and adapt security behaviours from one work location to another to minimise security-related stress at work. In contrast, employees who possess low levels of the challenge disposition are more likely to use avoidance as a coping strategy when they face stressful or unexpected security threats (Bartone et al., 2012).

Previous research on hardiness has shown that hardiness can be learned or transferred within groups or teams. Employees develop hardiness personality traits in socially-supportive interactions with colleagues who possess high levels of hardiness. Furthermore, these supportive interactions, as a potential resource, give employees an opportunity to share security knowledge which reduces the likelihood of security vulnerability within the organisation (Safa and von Solms, 2016). Employees with high levels of hardiness could mentor their colleagues in promoting problem-solving security behaviour and coping mechanisms through shared experiential feedback (Maddi, 2013). Therefore, promoting hardiness personality traits in employees can help build their resilient security behaviours, transforming their cognitive appraisal of security threats into a broader perspective leading to better security behaviours.

6.2.2 Habit and security-related stress

Habit significantly affects the security intentions of employees. This finding aligns with previous literature (Pahnila et al., 2007; Vance et al., 2012) on the role habit plays in employees' compliance with security policies. Employees will respond to security threats if they have a habit of taking security measures. For example, the use of BYOD at work allows employees to have some level of flexibility which could reduce their cognition of security threats when performing work tasks leading to automatic security response. Vance et al. (2012) showed that employees' security habit influences whether or not they feel they are subject to information security threats. Employees' strong habits are likely to override their security behavioural intentions, because of the automaticity of habits.

Security training helps employees develop security habits of complying with security policies (Puhakainen and Siponen, 2010). However, small businesses are less likely to have the expertise to implement a formal information security policy or have the financial resources to provide security training for their employees. One way to address this may be to break security procedures down into small routine activities, to encourage employees' formation of security habits. Studies on habit formation suggest that a simple action in a consistent context leads to a habit through association of cues (Gardner et al., 2012). The consistency of carrying out a security action needs to be internalised by employees for the formation of security habit. Employees can learn to associate a daily routine with security procedures when working from different locations such as launching a virtual private network (VPN) on their personal device when getting coffee.

Consistent with technostress studies, security-related *stress* in this study negatively influences employees' *attitude* toward security behaviour (Ayyagari et al., 2011; D'Arcy et al., 2014b; Lee et al., 2016). Stress in this context arises when employees have to meet security requirements such as the configuration of personal devices or authentication process before accessing organisational information assets. Employees may feel overwhelmed with the security demands that require them to continually configure their personal device to be compliant with the organisation's security procedures. SMEs as supply chain partners are often required to follow strict security procedures when they access partner organisation’s networks or information assets, that results in technostress. Consistent with previous studies (D’Arcy et al., 2014b), this study showed that employees working in stressful environments might put up resistance towards security policies as they may feel that security requirements increase their workload. Furthermore, continually dealing with stressful security requirements may weaken employees’ positive attitude towards security behaviours (D’Arcy and Lowry, 2017). Therefore, security policies and procedures across daily business processes need to be less complicated for employees to implement.

6.2.3 Threat appraisal

This study found employees’ threat appraisal process to be insignificant. This was unexpected because in PMT, an individual’s cognitive appraisal of a threat event leads to a change in behaviour. Prior studies have reported mixed findings regarding employees’ threat appraisals. The findings in this study shows that employees performing work tasks with BYOD did not feel that they were vulnerable to information security threats. Prior studies on *perceived vulnerability* had insignificant effects (Johnston and Warkentin, 2010; Vance et al., 2012) suggesting that employees perceived they were less likely to experience a security threat. One possible explanation could be because vulnerability is usually interpreted differently by employees based on their environment (Thompson et al., 2017). Attempting to motivate employees with fear to undertake security behaviours when accessing organisational networks may not be effective for BYOD used to access to organisational assets. One reason may be that employees often perceive that organisational information has no personal connection to them. Therefore, SMEs should encourage employees to take personal ownership of work tasks to motivate them to protect organisational information (Menard et al., 2018).

Perceived severity was insignificant in this study similar to Posey et al. (2015) and Thompson et al. (2017). In our scenario, respondents placed more importance on performing the work task to avoid sanctions from the manager instead of security risk. Employees often apply neutralisation techniques when completing a task and in the process, they fail to acknowledge or follow security procedures (Siponen and Vance, 2010). The strong influence of hardiness personality traits and habit may explain how employees evaluate the perceived threat in alternative locations of work. Employees with a high level of hardiness are confident that they can influence the security threat in alternative work locations.

6.2.4 Effect of social influence

In this study, *subjective norms* had little effect on employees' security intention. This finding shows that with the use of BYOD for work related tasks, SME employees are aware of expected security behaviour but are not motivated by the social relationships with managers or colleagues to engage in the appropriate security behaviour. SMEs do not have a strong hierarchical or formal authority structure. Therefore employees have more work autonomy that reduces the effect of social influence on employees' security behaviour (Anderson and Agarwal, 2010; Thompson et al., 2017). However, it is possible that the effect of social influence varies because employees are motivated to adjust their security behaviour based on the actual compliant behaviour of their colleagues rather than acting as managers expect (D'Arcy and Lowry, 2017).

6.3 Contributions to theory, research and practice

The findings in this study have important contributions to the information security literature: a multi-theory concept, the influence of hardiness personality traits, habit, stress and the effect of threat appraisal.

The findings contribute to behavioural information systems security theory by proposing a multi-theory concept that integrates PMT, TPB, habit, hardiness and stress in the context of SME employees' behavioural intentions.

The inclusion of *hardiness* personality traits strengthens our understanding of factors that influence positive security behaviours in employees. The findings show that there may be unknown psychological factors that employees can be encouraged to develop to motivate them to engage in positive security behaviour within the context of information security. Hardiness personality traits in this study provide insights into understanding how employees' levels of hardiness frame their security behaviour. The results show that all dimensions of hardiness: *commitment, control* and *challenge*, are important in determining employees' security behaviour.

This study expands the SME information security literature by evaluating factors such as *habit* and *stress*, in the context of BYOD used for working and anywhere working. Employees' stressful working conditions may lead to a habitual response because the automaticity of the response (habit) requires less cognitive effort to perform. This study shows that the automaticity of habit is important in explaining employees' security behaviour, especially in work locations where employees feel they are not subject to information security threats.

The findings on security-related stress emphasise that although employees enjoy the potential benefits and flexibility of BYOD and anywhere working, they still have to deal with techno-security stress which negatively affects their security behaviour. This study broadens the research on technostress and shows that security stressors are evolving with the workplace and technology and impacts employees' security behaviour negatively.

This study contributes to the literature on threat appraisal in information security. The *perceived severity* and *vulnerability* of threats did not affect employees' security behaviour. This shows that employees working anywhere using BYOD do not engage in a specific security behaviour as a response to fear because of the level of autonomy they have when using their personal device. If employees perceive that security threats will not harm them directly, the threat appraisal process will not affect their security intention.

The study has three practical implications. The first is that employees that exhibit high levels of the hardiness personality traits are resilient. Therefore, managers should review stressful security policies to encourage employees to build more resilient security behaviours especially among employees with low levels of hardiness. Management should consider the difference in hardiness levels among employees as input into the design of security policy development and training.

Second, habit's influence on employees' security behaviour shows that SME employees need to develop the habit of complying with security policies and carrying out security practices as automatic responses when working performing work tasks regardless of location. To facilitate employees' formation of the habit, IT managers need to create a favourable environment where employees feel motivated to comply with security policies.

Finally, managers should be aware that when designing security policies that fear does not motivate employees to comply. Therefore, security training and awareness should not focus on the threat. The emphasis should be on designing security training and awareness programs that develop the psychological capability of employees to reinforces positive security behaviour.

6.4 Summary

The results of the study show that psychological hardiness plays an important role in employees' security behavioural intention allowing them to take charge of their work location and influence events that may directly or indirectly affect them. The results show that an employees' security behaviour may change depending on their perception of security threats when performing work task and the security threat perceived at a location when working with BYOD.

Chapter 7: Conclusion

In Australia, three months after the notifiable data breaches (NDB) came into effect, 50 per cent of the breaches reported were attributed to human error (OAIC, 2018). Despite information security policies and regulations to guide employee access and handling of organisational data and information assets, security breaches are often caused by human error. In this study, a theoretical model was developed to investigate and explain the factors that may influence SME employees' security behaviours when working with personal devices from multiple work locations. SMEs constitute the largest number of businesses in the supply chain network and employ most of the working population in a growing economy. In 2018, NIST released an update to its cybersecurity framework, acknowledging the importance of securing the supply chain network and greatly expanding on the security requirements for supply chain risk management (NIST, 2018).

A review of the literature showed that the security threat landscape is constantly evolving because hackers are exploiting employee weaknesses within the security network and taking advantage of vulnerabilities relating to new technologies and different ways of working. A key component for mitigating cybersecurity breaches is to better understand employees' behaviour, particularly when working in different locations (Crossler et al., 2013). This study has contributed to our understanding of the security behaviours of SME employees using personal devices for work purposes from different work locations.

A theoretical model was developed using the theory of planned behaviour (TPB), protection motivation theory (PMT), habit, hardiness, and security-related stress. The model included nine main constructs: *hardiness, stress, habit, attitude, subjective norms, perceived severity, perceived vulnerability, security intention* and *security behaviour*. The empirical data collected and analysed was used to test the theoretical model, the results answered to the research question: *How do the type of work tasks and locations of work change SME employee security behaviours when using personal devices?* The findings showed that the level of hardiness personality traits an employee possesses may influence their habit, buffer or intensify stress and may cause them to change their security behaviour.

The emphasis was on the *hardiness* construct because hardiness had not been examined in the information security behaviour context. Hardiness is a personality characteristic that functions as resistance and buffers when people (employees) encounter stressful events (Kobasa, 1979).

Hardiness consists of three personality dispositions: *commitment, control* and *challenge*. *Commitment* refers to the belief of staying involved in situations no matter how bad instead of detachment and alienation. *Control* is the belief that the employee can turn stresses from a potential disaster into opportunities for growth. *Challenge* is an acceptance of stressful change as an opportunity to learn by trying to turn them to an advantage. Employees need to strongly possess all three dispositions of hardiness to turn stressors into advantages; this is particularly important for understanding security behaviours.

The hardiness personality traits are a significant predictor of security behaviours. In the model, hardiness personality traits comprising of the three dispositions had a significant influence on employees' attitude towards security. Employees with high levels of hardiness who develop strong tendencies towards commitment, control and challenge are better prepared to combat security threats and engage in positive security practices when working. Therefore, an understanding of an employee's level of hardiness is important for predicting their security behaviour.

Hardiness is a malleable trait and can be learned at any time in life through training and mentoring (Maddi, 2013). This finding provides management with insights into how hardiness could be developed through targeted interventions building at the dispositional levels to strengthen employees' hardiness traits. SME employees who develop strong hardiness traits and strategies are problem solvers, exhibit secured behavioural traits and as managers, they mentor hardiness in teams they manage leading to better security behaviours.

Habit and security-related *stress* were high predictors of employee security behaviours and should be considered along with hardiness. The strength of habit varies in different work locations. Habitual behaviours become dominant where the work tasks and/or location of work require less cognitive effort from the employee. It is essential for SME employee to develop positive security habits, especially when using personal devices for work purposes. The use of personal devices at work blur the line between private and professional environments which may lead employees to exhibit automatic behaviour (habit) when a memory cue presents itself. Employees dealing with stressful workloads from alternative work locations may perform work tasks habitually paying less attention to new information that may signal security threats.

Management can promote employee security habit formation by creating security policies that require employees to consistently perform the same simple security procedures until the act is associated with a cue for action. Security-related stress, on the other hand, will increase employees' cognitive load causing them to engage in habitual behaviours that require less cognitive effort. Management needs to consider that employees may not possess the security skills to ensure that security procedures are followed to protect organisational assets if they are too complex.

One unusual finding in the study was the weakness of security threats. Employees usually engage a behavioural response when they feel a security threat is directed towards them. In this study, employees use of BYOD for work resulted in the externalisation of information security threats. Management should ensure employees are aware of the contents of security and BYOD policies by creating stress-free procedures to motivate security behaviours when using BYOD from different work locations.

Practitioners and academics can draw on the findings of this study. Practitioners can leverage on the benefits of hardiness to develop appropriate security behaviours among employees. IT managers should get employees into the habit of following security policies to improve their security behaviours irrespective of work locations. Management should communicate regular security updates to employees and encourage feedback to help redesign and implement security requirements.

Academics can explore the hardiness construct with other theories and variables in future information security studies. Further studies can investigate the mediating or moderating effect of hardiness on security behaviours. Finally, fear appeals may not always influence employee security behaviours; future studies should investigate threat appraisal in the context where employees have high workplace autonomy such as anywhere working.

7.1 Limitations and future studies

This study provides insights into the role hardiness, habit, stress and threats play in determining an employee's security behaviour. Hardiness was the strongest determinant of SME employee security behaviour, enabling them to buffer stressful work and security requirements.

The theoretical model focused on constructs from the threat appraisal process of the PMT model. Therefore, the model did not include fear in the threat appraisal process or the other constructs in the coping appraisal process (Posey et al., 2015). Future research could explore the role of hardiness in the cognitive mediating process with the full version of the PMT theoretical model.

The measures of hardiness used in the study consisted of an equal number of positively and negatively worded questions. The negative indicators of hardiness did not allow for accurate measures in the study. Some researchers have suggested that the hardiness scale should be modified to include more positive indications for each of the dispositions: commitment, control and challenge (Funk, 1992; Kardum et al., 2012). Further studies on hardiness within the information security domain could consider testing other measures of hardiness. Studies could also explore studying hardiness with security behaviours or other variables of interest and the moderating and/or mediating effect of hardiness with an emphasis on information security behaviours. Finally, given the structure of hardiness, security behavioural researchers could develop targeted measures of commitment, control and challenge concerning information systems security behaviour.

A possible limitation was the use of online panels and the restriction of MTurk workers to only the United States. Steelman et al. (2014) recommended that researchers use US samples on the MTurk website because they were found to be more viable. However, there was the risk of the respondent's use of VPNs to mask IP addresses. Therefore, future research should use other samples from more traditional data sources to validate the results of the study.

Future studies should empirically test and validate the theoretical model using data from other sources such as security professionals or home users. A qualitative approach using semi-structured interviews could be used to obtain a deeper understanding of employees' hardiness personality traits in relation to security behaviour and coping mechanism to a security threat.

Finally, a longitudinal study could be conducted to observe how habit influences security intentions or not and evolves into security behaviour over time. Researchers could monitor how employees' new security habit develops into an automatic behavioural response to better understand security behaviours.

References

Agudelo, C.A., Bosua, R., Ahmad, A., Maynard, S.B., 2015. Understanding Knowledge Leakage & BYOD (Bring Your Own Device): A Mobile Worker Perspective 13.

Ajzen, I., 2011. The theory of planned behavior: Reactions and reflections. Psychology and Health 26, 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Ajzen, I., 1991. The theory ocybf planned behavior. Organizational behavior and human decision processes 50, 179–211.

Ajzen, I., 1985. From Intentions to Actions: A Theory of Planned Behavior, in: Kuhl, J., Beckmann, J. (Eds.), Action Control: From Cognition to Behavior. Springer, Heidelberg, pp. 11–39. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I., Fishbein, M., 2000. Attitudes and the Attitude-Behavior Relation: Reasoned and Automatic Processes. European Review of Social Psychology 11, 1–33. https://doi.org/10.1080/14792779943000116

Akhunzada, A., Sookhak, M., Anuar, N.B., Gani, A., Ahmed, E., Shiraz, M., Furnell, S., Hayat, A., Khurram Khan, M., 2015. Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions. Journal of Network and Computer Applications 48, 44–57. https://doi.org/10.1016/j.jnca.2014.10.009

Al-Ahmad, W., Mohammad, B., 2013. Addressing Information Security Risks by Adopting Standards. International Journal of Information Security Science 2, 28–43.

Al-Isma’ili, S., Li, M., Shen, J., He, Q., 2016. Cloud computing adoption determinants: an analysis of Australian SMEs. Conference on Information Systems 2016 Proceedings 1–17.

Allen, T.D., Golden, T.D., Shockley, K.M., 2015. How Effective Is Telecommuting? Assessing the Status of Our Scientific Findings. Psychological Science in the Public Interest 16, 40–68.

Alshamaila, Y., Papagiannidis, S., Li, F., 2013. Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. Journal of Enterprise Information Management 26, 250–275. https://doi.org/10.1108/17410391311325225

Al-Suqri, M.N., Al-Kharusi, R.M., 2015. Information Seeking Behavior and Technology Adoption: Theories and Trends, Advances in Knowledge Acquisition, Transfer, and Management. IGI Global. https://doi.org/10.4018/978-1-4666-8156-9

Anderson, C.L., Agarwal, R., 2010. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly 34, 613–643. https://doi.org/10.2307/25750694

Antonucci, D., 2017. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. John Wiley & Sons, New Jersey.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Ashford, W., 2017. New TalkTalk fine takes total for poor data protection to £500,000 [WWW Document]. ComputerWeekly.com. URL https://www.computerweekly.com/news/450424226/New-TalkTalk-fine-takes-total-for-poor-data-protection-to-500000 (accessed 4.24.18).

Australian Bureau of Statistics, 2017. Selected Characteristics of Australian Business [WWW Document]. URL http://www.abs.gov.au/ausstats/abs@.nsf/mf/8167.0 (accessed 9.29.17).

Ayyagari, R., 2012. Impact of information overload and task-technology fit on technostress, in: Proceedings of the Southern Association for Information Systems Conference. pp. 18–22.

Ayyagari, R., Grover, V., Purvis, R., 2011. Technostress: Technological Antecedents & Implications. MIS Quarterly 35, 831–858.

Bansal, G., Zahedi, F. "Mariam", Gefen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems 49, 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Bartone, P.T., 2012. Social and organizational influences on psychological hardiness: How leaders can increase stress resilience. Security Informatics 1, 21. https://doi.org/10.1186/2190-8532-1-21

Bartone, P.T., 2006. Resilience Under Military Operational Stress: Can Leaders Influence Hardiness? Military Psychology 18, S131–S148. https://doi.org/10.1207/s15327876mp1803s_10

Bartone, P.T., 1991. Development and Validation of a Short Hardiness Measure. Annual Convention of the American Psychological Society.

Bartone, P.T., Hystad, S.W., Eid, J., Brevik, J.I., 2012. Psychological hardiness and coping style as risk/resilience factors for alcohol abuse. Military Medicine 177, 517–524.

Bartone, P.T., Roland, R.R., Picano, J.J., Williams, T.J., 2008. Psychological Hardiness Predicts Success in US Army Special Forces Candidates. International Journal of Selection and Assessment 16, 78–81. https://doi.org/10.1111/j.1468-2389.2008.00412.x

Bartone, P.T., Ursano, R.J., Wright, K.M., Ingraham, L.H., 1989. The impact of a military air disaster on the health of assistance workers: A prospective study. The Journal of Nervous and Mental Disease, 1279 177, 317–328.

Bayrak, T., 2012. IT support services for telecommuting workforce. Telematics and Informatics 29, 286–293. https://doi.org/10.1016/j.tele.2011.10.002

Bentley, T., 2013. Future of work programme: Trans-Tasman telework survey [WWW Document]. URL http://apo.org.au/node/36225 (accessed 3.27.18).

Bentley, T.A., Teo, S.T.T., McLeod, L., Tan, F., Bosua, R., Gloet, M., 2016. The role of organisational support in teleworker wellbeing: A socio-technical systems approach. Applied Ergonomics 52, 207–215. https://doi.org/10.1016/j.apergo.2015.07.019

Blount, Y., 2017. Management Skills and Capabilities in an Era of Technology Disruption, in: Blount, Y., Gloet, M. (Eds.), Anywhere Working and the New Era of Telecommuting, Management Skills and Capabilities in an Era of Technology Disruption. IGI Global. https://doi.org/10.4018/978-1-5225-2328-4

Blount, Y., 2015a. Pondering the Fault Lines of Anywhere Working (Telework, Telecommuting): A Literature Review. Foundations and Trends in Information Systems 1, 163–276. https://doi.org/10.1561/2900000001

Blount, Y., 2015b. Managing the invisible employee: Productivity and availability. Governance Directions 67, 365.

Boer, H., Seydel, E.R., 1996. Protection Motivation Theory, in: Conner, M., Norman, P. (Eds.), Predicting Health Behaviour: Research and Practice with Social Cognition Models. Open University Press, Buckingham, pp. 95–120.

Bohannon, J., 2011. Social Science for Pennies. Science 334, 307–307. https://doi.org/10.1126/science.334.6054.307

Botta, A., de Donato, W., Persico, V., Pescapé, A., 2016. Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems 56, 684–700. https://doi.org/10.1016/j.future.2015.09.021

Boudreau, M.-C., Gefen, D., Straub, D.W., 2001. Validation in Information Systems Research: A State-of-the-Art Assessment. MIS Quarterly 25, 1. https://doi.org/10.2307/3250956

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly 34, 523-A7.

Burns, A.J., Posey, C., Roberts, T.L., Benjamin Lowry, P., 2017. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. Computers in Human Behavior 68, 190–209. https://doi.org/10.1016/j.chb.2016.11.018

Butler, S.E., Aasheim, C., Williams, S., 2007. Does Telecommuting Improve Productivity? Communications of the ACM 50, 101–103.

Chandler, J., Shapiro, D., 2016. Conducting Clinical Research Using Crowdsourced Convenience Samples. Annual Review of Clinical Psychology 12, 53–81. https://doi.org/10.1146/annurev-clinpsy-021815-093623

Chen, Y., Ramamurthy, K., Wen, K.-W., 2012. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? Journal of Management Information Systems 29, 157–188. https://doi.org/10.2753/MIS0742-1222290305

Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q., 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security 39, 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Cheng, L., Liu, F., Yao, D. (Daphne), 2017. Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 7. https://doi.org/10.1002/widm.1211

Cheung, C., Limayem, M., 2005. The role of habit in information systems continuance: examining the evolving relationship between intention and usage. ICIS 2005 Proceedings 39.

Chin, W., 1998. The Partial Least Squares Approach to Structural Equation Modeling. Modern Methods for Business Research 295–336.

Cisco, 2017. Cisco 2017 Midyear Cybersecurity Report.

Cohen, J., 1988. Statistical power analysis for the behavioral sciences, 2nd ed. L. Erlbaum Associates, Hillsdale, N.J.

Cram, A.W., Proudfoot, J.G., D'Arcy, J., 2017. Organisational information security policies: a review and reserarch framework. European Journal of Information Systems 1–37. https://doi.org/10.1057/s41303-017-0059-9

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Computers & Security 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Crossler, R.E., Long, J.H., Loraas, T.M., Trinkle, B.S., 2014. Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-

Behavior Gap. Journal of Information Systems 28, 209–226. https://doi.org/10.2308/isys-50704

Crump, M.J.C., McDonnell, J.V., Gureckis, T.M., 2013. Evaluating Amazon’s Mechanical Turk as a Tool for Experimental Behavioral Research. PLOS ONE 8, e57410. https://doi.org/10.1371/journal.pone.0057410

D’Arcy, J., Devaraj, S., 2012. Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. Decision Sciences 43, 1091–1124. https://doi.org/10.1111/j.1540-5915.2012.00383.x

D’Arcy, J., Gupta, A., Tarafdar, M., Turel, O., 2014a. Reflecting on the" Dark Side" of Information Technology Use. CAIS 35, 5.

D’Arcy, J., Herath, T., Shoss, M.K., 2014b. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal of Management Information Systems 31, 285–318. https://doi.org/10.2753/MIS0742-1222310210

D’Arcy, J., Hovav, A., 2009. Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. Journal of Business Ethics 89, 59–71. https://doi.org/10.1007/s10551-008-9909-7

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, 79–98. https://doi.org/10.1287/isre.1070.0160

D’Arcy, J., Lowry, P.B., 2017. Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal 1–27. https://doi.org/10.1111/isj.12173

De Haes, S., Van Grembergen, W., Debreceny, R.S., 2015. COBIT as Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems 27, 307–324. https://doi.org/10.2308/isys-50422

Deloitte, 2017. Deloitte Statement on Cyber Incident [WWW Document]. Deloitte. URL https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html (accessed 6.6.18).

Department for Business, Energy & Industrial Strategy, 2017. Business Population Estimates for the UK and Regions 2017. London.

Dhillon, G., Backhouse, J., 2000. Technical opinion: Information system security management in the new millennium. Communications of the ACM 43, 125–128.

Drucker, P.F., 1999. Knowledge-worker productivity: The biggest challenge. California Management Review 41, 79–94.

EUGDPR, 2018. Key Changes with the General Data Protection Regulation [WWW Document]. EU GDPR Portal. URL http://eugdpr.org/the-regulation.html (accessed 3.27.18).

EY, 2017. “WannaCry” ransomware attack: Technical intelligence analysis. Ernst & Young, UK.

Fishbein, M., Ajzen, I., 1975. Belief, attitude, intention, and behavior: An introduction to theory and research. Addison-Wesley, Reading, MA.

Florian, V., Mikulincer, M., Taubman, O., 1995. The role of hardiness in stress and illness: An exploration of the effect of negative affectivity and gender. Journal of Personality and Social Psychology 68, 687–695.

Flowerday, S.V., Tuyikeze, T., 2016. Information security policy development and implementation: The what, how and who. Computers & Security 61, 169–183. https://doi.org/10.1016/j.cose.2016.06.002

Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology 30, 407–429.

Funk, S.C., 1992. Hardiness: A review of theory and research. Health Psychology 11, 335.

Funk, S.C., Houston, B.K., 1987. A Critical Analysis of the Hardiness Scale’s Validity and Utility. Journal of Personality and Social Psychology 53, 572–578.

Furnell, S., Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. Computers & Security 31, 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Gardner, B., Lally, P., Wardle, J., 2012. Making health habitual: the psychology of ‘habit-formation’ and general practice. Br J Gen Pract 62, 664–666. https://doi.org/10.3399/bjgp12X659466

Gefen, D., Straub, D., 2005. A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example. Communications of the AIS 91–109.

Golden, T.D., 2009. Applying technology to work: toward a better understanding of telework. Organization Management Journal 6, 241–250. https://doi.org/10.1057/omj.2009.33

Graber, S., 2015. Why Remote Work Thrives in Some Companies and Fails in Others [WWW Document]. Harvard Business Review. URL https://hbr.org/2015/03/why-remote-work-thrives-in-some-companies-and-fails-in-others (accessed 8.26.17).

Greene, C., Myerson, J., 2011. Space for thought: designing for knowledge workers. Facilities 29, 19–30. https://doi.org/10.1108/02632771111101304

Guo, K.H., 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security 32, 242–251. https://doi.org/10.1016/j.cose.2012.10.003

Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E., 2011. Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. Journal of Management Information Systems 28, 203–236. https://doi.org/10.2753/MIS0742-1222280208

Hair, J.F., Celsi, M.W., Money, A.H., Samouel, P., Page, M.J., 2016. Essentials of Business Research Methods, Third. ed. Routledge, New York.

Hair, J.F., 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 117, 442–458. https://doi.org/10.1108/IMDS-04-2016-0130

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., 2014a. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Sage, Thousand Oaks.

Hair, J.F., Ringle, C.M., Sarstedt, M., 2011. PLS-SEM: Indeed a Silver Bullet. The Journal of Marketing Theory and Practice 19, 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hair, J.F., Sarstedt, M., Hopkins, L., G. Kuppelwieser, V., 2014b. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. European Business Review 26, 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Hair, J.F., Sarstedt, M., Ringle, C.M., Mena, J.A., 2012. An assessment of the use of partial least squares structural equation modeling in marketing research. Journal of the Academy of Marketing Science 40, 414–433. https://doi.org/10.1007/s11747-011-0261-6

Healy, J., Nicholson, D., Pekarek, A., 2017. Should we take the gig economy seriously? Labour & Industry: a journal of the social and economic relations of work 27, 232–248. https://doi.org/10.1080/10301763.2017.1377048

Henke, R.M., Benevent, R., Schulte, P., Rinehart, C., Crighton, K.A., Corcoran, M., 2016. The Effects of Telecommuting Intensity on Employee Health. American Journal of Health Promotion 30, 604–612. https://doi.org/10.4278/ajhp.141027-QUAN-544

Henseler, J., Hubona, G., Ray, P.A., 2017. Partial Least Squares Path Modeling: Updated Guidelines, in: Latan, H., Noonan, R. (Eds.), Partial Least Squares Path Modeling. Springer International Publishing, Cham, pp. 19–39. https://doi.org/10.1007/978-3-319-64069-3_2

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. of the Acad. Mark. Sci. 43, 115–135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Sarstedt, M., 2013. Goodness-of-fit indices for partial least squares path modeling. Computational Statistics 28, 565–580. https://doi.org/10.1007/s00180-012-0317-1

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18, 106–125.

Holtgrewe, U., 2014. New new technologies: the future and the present of work in information and communication technology. New Technology, Work and Employment 29, 9–24. https://doi.org/10.1111/ntwe.12025

Humphry, J., 2013. Yahoo brings workers back into the office but leaves real issues out in the cold [WWW Document]. The Conversation. URL http://theconversation.com/yahoo-brings-workers-back-into-the-office-but-leaves-real-issues-out-in-the-cold-12536 (accessed 2.26.18).

Huong Tran, T.T., Childerhouse, P., Deakins, E., 2016. Supply chain information sharing: challenges and risk mitigation strategies. Journal of Manufacturing Technology Management 27, 1102–1126. https://doi.org/10.1108/JMTM-03-2016-0033

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

Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security 31, 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Innovation Value Institute, 2016. IT Capability Maturity Framework-Information Security Management.

ISF, 2016. The ISF Standard of Good Practice for Information Security.

ISO, 2016. International Standard ISO/IEC 27000. Switzerland.

Jang-Jaccard, J., Nepal, S., 2014. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, Special Issue on Dependable and Secure Computing 80, 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jarvis, C., MacKenzie, S., M Podsakoff, P., 2003. A Critical Review of Construct Indicators and Measurement Model Specification in Marketing and Consumer Research. Journal of Consumer Research 30, 199–218. https://doi.org/10.1086/376806

Johns, T., Gratton, L., 2013. The third wave of virtual work. Harvard Business Review 91, 66–73.

Johnston, A.C., Warkentin, M., 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34, 549-A4.

Johnston, A.C., Warkentin, M., McBride, M., Carter, L., 2016. Dispositional and situational factors: influences on information security policy violations. European Journal of Information Systems 25, 231–251.

Johnston, A.C., Warkentin, M., Siponen, M., 2015. An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. MIS Quarterly 39, 113-A7.

Kajzer, M., D'Arcy, J., Crowell, C.R., Striegel, A., Van Bruggen, D., 2014. An exploratory investigation of message-person congruence in information security awareness campaigns. Computers & Security 43, 64–76. https://doi.org/10.1016/j.cose.2014.03.003

Kardum, I., Hudek-Knežević, J., Krapić, N., 2012. The structure of hardiness, its measurement invariance across gender and relationships with personality traits and mental health outcomes. Psihologijske teme 21, 487–507.

Kobasa, S.C., 1979. Stressful life events, personality, and health: an inquiry into hardiness. Journal of Personality and Social Psychology 37, 1–11.

Kobasa, S.C., Maddi, S.R., Kahn, S., 1982. Hardiness and health: a prospective study. Journal of personality and social psychology 42, 168–177.

Kotey, B.A., 2017. Flexible working arrangements and strategic positions in SMEs. Personnel Review 46, 355–370. https://doi.org/10.1108/PR-04-2015-0089

Kotulic, A.G., Clark, J.G., 2004. Why there aren't more information security research studies. Information & Management 41, 597–607. https://doi.org/10.1016/j.im.2003.08.001

Kurpjuhn, T., 2015. The SME security challenge. Computer Fraud & Security 2015, 5–7. https://doi.org/10.1016/S1361-3723(15)30017-8

Layton, R., Watters, P.A., 2014. A methodology for estimating the tangible cost of data breaches. Journal of Information Security and Applications 19, 321–330. https://doi.org/10.1016/j.jisa.2014.10.012

Lee, C., Lee, C.C., Kim, S., 2016. Understanding information security stress: Focusing on the type of information security compliance activity. Computers & Security 59, 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Limayem, M., Hirt, S.G., Cheung, C.M., 2007. How habit limits the predictive power of intention: The case of information systems continuance. MIS quarterly 31, 705–737.

Low, C., Chen, Y., Wu, M., 2011. Understanding the determinants of cloud computing adoption. Industrial Management & Data Systems 111, 1006–1023. https://doi.org/10.1108/02635571111161262

Lowry, P.B., D'Arcy, J., Hammer, B., Moody, G.D., 2016. "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. The Journal of Strategic Information Systems 25, 232–240. https://doi.org/10.1016/j.jsis.2016.06.002

Lowry, P.B., Gaskin, J., 2014. Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. IEEE Transactions on Professional Communication 57, 123–146.

MacKenzie, S.B., Podsakoff, P.M., Jarvis, C.B., 2005. The Problem of Measurement Model Misspecification in Behavioural and Organizational Research and Some Recommended Solutions. Journal of Applied Psychology 90, 710–730. https://doi.org/0.1037/0021-9010.90.4.710

MacKenzie, S.B., Podsakoff, P.M., Podsakoff, N.P., 2011. Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. MIS Quarterly 35, 293–334.

Maddi, S., 2013. Personal Hardiness as the Basis for Resilience, in: Hardiness. Springer Netherlands, Dordrecht, pp. 7–17. https://doi.org/10.1007/978-94-007-5222-1_2

Maddi, S.R., Harvey, R.H., Khoshaba, D.M., Lu, J.L., Persico, M., Brow, M., 2006. The Personality Construct of Hardiness: III. Relationships With Repression, Innovativeness, Authoritarianism, and Performance. Journal of Personality 74, 575–598. https://doi.org/10.1111/j.1467-6494.2006.00385.x

Maddi, S.R., Khoshaba, D.M., 1994. Hardiness and Mental Health. Journal of Personality Assessment 63, 265–274. https://doi.org/10.1207/s15327752jpa6302_6

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: Effects of technostress and switching stress. Information Systems Journal 25, 275–308. https://doi.org/10.1111/isj.12068

Mansfield-Devine, S., 2016. Securing small and medium-size businesses. Network Security 2016, 14–20. https://doi.org/10.1016/S1353-4858(16)30070-8

Marrone, M., Gacenga, F., Cater-Steel, A., Kolbe, L., 2014. IT service management: A cross-national study of ITIL adoption. Communications of the Association for Information Systems 34.

Martin, B.H., MacDonnell, R., 2012. Is telework effective for organizations?: A meta-analysis of empirical research on perceptions of telework and organizational outcomes. Management Research Review 35, 602–616. https://doi.org/10.1108/01409171211238820

Martin, J.A., 2017. 10 things you need to know about the security risks of wearables [WWW Document]. CIO. URL https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html (accessed 10.19.17).

McCrank, J., Finkle, J., 2018. Equifax breach could be most costly in corporate history. Reuters.

Menard, P., Bott, G.J., Crossler, R.E., 2017. User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. Journal of Management Information Systems 34, 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Menard, P., Warkentin, M., Lowry, P.B., 2018. The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. Computers & Security 75, 147–166. https://doi.org/10.1016/j.cose.2018.01.020

Middleton, C., Scheepers, R., Tuunainen, V.K., 2014. When mobile is the norm: researching mobile information systems and mobility as post-adoption phenomena. European Journal of Information Systems 23, 503–512. https://doi.org/10.1057/ejis.2014.21

Moody, G.D., Siponen, M., Pahnila, S., 2018. Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly 42, 285-A22.

Moore, J.E., 2000. One Road to Turnover: An Examination of Work Exhaustion in Technology Professionals. MIS Quarterly 24, 141. https://doi.org/10.2307/3250982

Morganson, V.J., Major, D.A., Oborn, K.L., Verive, J.M., Heelan, M.P., 2010. Comparing telework locations and traditional work arrangements: Differences in work-life balance support, job satisfaction, and inclusion. Journal of Managerial Psychology 25, 578–595. https://doi.org/10.1108/02683941011056941

Mouton, F., Leenen, L., Venter, H.S., 2016. Social engineering attack examples, templates and scenarios. Computers & Security 59, 186–209. https://doi.org/10.1016/j.cose.2016.03.004

NCSL, 2018. Security Breach Notification Laws [WWW Document]. National Conference of State Legislatures. URL http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (accessed 4.24.18).

Newsted, P.R., Huff, S.L., Munro, M.C., 1998. Survey Instruments in Information Systems. MIS Quarterly 22, 553–553.

Ng, Z.X., Ahmad, A., Maynard, S.B., 2013. Information security management: Factors that influence security investments in SMES. Australian Information Security Management Conference.

Nguyen, T.H., Newby, M., Macaulay, M.J., 2015. Information Technology Adoption in Small Business: Confirmation of a Proposed Framework. Journal of Small Business Management 53, 207–227. https://doi.org/10.1111/jsbm.12058

NHMRC, 2015. National Statement on Ethical Conduct in Human Research. The National Health and Medical Research Council, the Australian Research Council and the Australian Vice-Chancellors' Committee. Commonwealth of Australia, Canberra E72, 101.

NIST, 2018. NIST Cybersecurity Framework (No. v1.1). National Institute of Standards and Technology, USA.

NIST, 2013. Guidelines for Managing the Security of Mobile Devices in the Enterprise.

NIST, 2011. The NIST definition of cloud computing. NIST SP 800-145 7.

NZ Herald, 2018. Small and medium-sized NZ firms unprepared for cyber attacks: Experts. NZ Herald.

OAIC, 2018. Notifiable Data Breaches Quarterly Statistics Report: January 2018-March 2018. Office of the Australian Information Commissioner.

OAIC, 2014. Telstra breaches privacy of 15,775 customers - Office of the Australian Information Commissioner (OAIC) [WWW Document]. URL /media-and-speeches/media-releases/telstra-breaches-privacy-of-15-775-customers (accessed 7.16.18).

Office of Advocacy, 2017. United States Small Business Profiles. United States Small Business Administration 208.

Olalere, M., Abdullah, M.T., Mahmod, R., Abdullah, A., 2015. A review of bring your own device on security issues. Sage Open 5, 1–11.

Orbell, S., Verplanken, B., 2015. The strength of habit. Health Psychology Review 9, 311–317. https://doi.org/10.1080/17437199.2014.992031

Ortiz de Guinea, A., Markus, M.L., 2009. Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use. Mis Quarterly 433–444.

Pahnila, S., Siponen, M., Mahmood, A., 2007. Employees' behavior towards IS security policy compliance, in: System Sciences, 2007. HICSS 2007. 40Th Annual Hawaii International Conference On. IEEE, pp. 156b–156b.

PCI-DSS, 2016. Payment Card Industry (PCI) Data Security Standard.

Peterson, S.J., Luthans, F., Avolio, B.J., Walumbwa, F.O., Zhang, Z., 2011. Psychological Capital and Employee Performance: A Latent Growth Modeling Approach. Personnel Psychology 64, 427–450. https://doi.org/10.1111/j.1744-6570.2011.01215.x

Pham, H., Brennan, L., Richardson, J., 2017. Review of Behavioural Theories in Security Compliance and Research Challenge. Proceedings of the Informing Science and Information Technology Education Conference 65–76.

Podsakoff, P.M., MacKenzie, S.B., Jeong-Yeon Lee, Podsakoff, N.P., 2003. Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. Journal of Applied Psychology 88, 879.

Podsakoff, P.M., MacKenzie, S.B., Podsakoff, N.P., 2012. Sources of Method Bias in Social Science Research and Recommendations on How to Control It. Annual Review of Psychology 63, 539–569. https://doi.org/10.1146/annurev-psych-120710-100452

Pogarsky, G., 2004. Projected Offending and Contemporaneous Rule-Violation: Implications for Heterotypic Continuity. Criminology 42, 111–138.

Ponemon, 2018. 2018 Cost of Data Breach Study (Research). USA.

Posey, C., Roberts, T.L., Lowry, P.B., 2015. The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. Journal of Management Information Systems 32, 179–214. https://doi.org/10.1080/07421222.2015.1138374

Privacy Amendment Act, 2017. Privacy Amendment (Notifiable Data Breaches) Act 2017 (No. 12,2017). Australia.

Puhakainen, P., Siponen, M., 2010. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly 34, 767-A4.

PWC, 2018. Global State of Information Security Survey 2018. PricewaterhouseCoopers.

Pyöriä, P., 2011. Managing telework: risks, fears and rules. Management Research Review 34, 386–399. https://doi.org/10.1108/01409171111117843

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, 417–433.

Recker, J., 2013. Scientific Research in Information Systems. Springer, Heidelberg. https://doi.org/10.1007/978-3-642-30048-6

Renaud, K., 2016. How smaller businesses struggle with security advice. Computer Fraud & Security 2016, 10–18. https://doi.org/doi.org/10.1016/S1361-3723(16)30062-8

Riedl, R., Kindermann, H., Aulnger, A., Javor, A., 2012. Technostress from a Neurobiological Perspective. Business & Information Systems Engineering 2, 61–69. https://doi.org/10.1007/s12599-012-0207-7

Ringle, C.M., Wende, S., Becker, J.-M., 2015. SmartPLS 3. Boenningstedt: SmartPLS GmbH.

Rocha Flores, W., Ekstedt, M., 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security 59, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation 153–177.

Rogers, R.W., 1975. A Protection Motivation Theory of fear appeals and attitude change. Journal of Psychology, 91 93–114.

Sadiku, M.N.O., Musa, S.M., Momoh, O.D., 2014. Cloud Computing: Opportunities and Challenges. IEEE Potentials 33, 34–36. https://doi.org/10.1109/MPOT.2013.2279684

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

Safa, N.S., von Solms, R., Furnell, S., 2016. Information security policy compliance model in organizations. Computers & Security 56, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

SANS, 2018. CIS Controls Measures and Metrics V7.

SANS, 2016a. IT security spending trends. SANS Institute.

SANS, 2016b. Information Security Policy Templates [WWW Document]. URL https://www.sans.org/security-resources/policies (accessed 2.28.18).

Saunders, M., Lewis, P., Thornhill, A., 2016. Research Methods for Business Students, 7th ed. Pearson, Essex, London.

Sebescen, N., Vitak, J., 2017. Securing the human: Employee security vulnerability risk in organizational settings. Journal of the Association for Information Science and Technology 68, 2237–2247. https://doi.org/10.1002/asi.23851

Sekaran, U., Bougie, R., 2013. Research Methods for Business, Sixth. ed. Wiley, United Kingdom.

Shropshire, J., Warkentin, M., Sharma, S., 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security 49, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Singh, A.N., Picot, A., Kranz, J., Gupta, M.P., Ojha, A., 2013. Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. Global Journal of Flexible Systems Management 14, 225–239. https://doi.org/10.1007/s40171-013-0047-4

Siponen, M., 2006. Information security standards focus on the existence of process, not its content. Communications of the ACM 49, 97. https://doi.org/10.1145/1145287.1145316

Siponen, M., Adam Mahmood, M., Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. Information & Management 51, 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Vance, A., 2014. Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. European Journal of Information Systems 23, 289–305. https://doi.org/10.1057/ejis.2012.59

Siponen, M., Vance, A., 2010. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly 34, 487-A12.

Sommestad, T., Karlzén, H., Hallberg, J., 2015. A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy (IJISP) 9, 26–46.

Soomro, Z.A., Shah, M.H., Ahmed, J., 2016. Information security management needs more holistic approach: A literature review. International Journal of Information Management 36, 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Spanos, G., Angelis, L., 2016. The impact of information security events to the stock market: A systematic literature review. Computers & Security 58, 216–229. https://doi.org/10.1016/j.cose.2015.12.006

Steelman, Z.R., Hammer, B.I., Limayem, M., 2014. Data Collection in the Digital Age: Innovative Alternatives to Student Samples. MIS Quarterly 38, 355-A20.

Straub, D., Boudreau, M.-C., Gefen, D., 2004. Validation guidelines for IS positivist research. The Communications of the Association for Information Systems 13, 63.

Straub, D.W., 1989. Validating Instruments in MIS Research. MIS Quarterly 13, 147–169.

Street, C.T., Gallupe, B., Baker, J., 2017. Strategic Alignment in SMEs: Strengthening Theoretical Foundations. Communications of the Association for Information Systems 40, 420–442. https://doi.org/10.17705/1CAIS.04020

Susanto, H., Almunawar, M.N., Tuan, Y.C., 2011. Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences 11, 23–29.

Symantec, 2018. Internet Security Threat Report (No. 23).

Symantec, 2017. Internet Security Threat Report (No. 22).

Tarafdar, M., Tu, Q., Ragu-Nathan, B., Ragu-Nathan, T., 2007. The Impact of Technostress on Role Stress and Productivity. Journal of Management Information Systems 24, 301–328. https://doi.org/10.2753/MIS0742-1222240109

Taylor, F.W., 1911. The Principles of Scientific Management. Harper, New York.

Telstra, 2018. Telstra Security Report 2018.

The Guardian, 2017. Deloitte hit by cyber-attack revealing clients' secret emails. The Guardian.

Thompson, N., McGill, T.J., Wang, X., 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. Computers & Security 70, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

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

UPS Capital, 2017. Cyber Security.

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

Vandelannoitte, A.L., 2015. Managing BYOD: how do organizations incorporate user-driven IT innovations? Info Technology & People 28, 2–33. https://doi.org/10.1108/ITP-11-2012-0129

Verizon, 2018. 2018 Data Breach Investigations Report (11th), Data breach investigations report. United States.

Verplanken, B., Aarts, H., 1999. Habit, Attitude, and Planned Behaviour: Is Habit an Empty Construct or an Interesting Case of Goal-directed Automaticity? European Review of Social Psychology 10, 101–134. https://doi.org/10.1080/14792779943000035

Verplanken, B., Orbell, S., 2003. Reflections on past behavior: A self-report index of habit strength. Journal of Applied Social Psychology 33, 1313–1330.

Vilhelmson, B., Thulin, E., 2016. Who and where are the flexible workers? Exploring the current diffusion of telework in Sweden. New Technology, Work and Employment 31, 77–96. https://doi.org/10.1111/ntwe.12060

von Solms, B., von Solms, R., 2005. From information security to…business security? Computers & Security 24, 271–273. https://doi.org/10.1016/j.cose.2005.04.004

Wang, J., Gupta, M., Rao, H.R., 2015. Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. MIS Quarterly 39, 91-A7.

Weeger, A., Wang, X., Gewald, H., 2016. It Consumerization: Byod-Program Acceptance and its Impact on Employer Attractiveness. Journal of Computer Information Systems 56, 1–10. https://doi.org/10.1080/08874417.2015.11645795

Weller, C., 2017. IBM was a pioneer in the work-from-home revolution -- now it’s cracking down | Business Insider [WWW Document]. URL https://www.businessinsider.com.au/ibm-slashes-work-from-home-policy-2017-3?r=US&IR=T (accessed 2.26.18).

Whitman, M.E., Mattord, H.J., 2012. Information Security Governance for the Non-Security Business Executive. Journal of Executive Education 11.

Willison, R., Warkentin, M., Johnston, A.C., 2016. Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. Info Systems J n/a-n/a. https://doi.org/10.1111/isj.12129

Wojcak, E., Bajzikova, L., Sajgalikova, H., Polakova, M., 2016. How to Achieve Sustainable Efficiency with Teleworkers: Leadership Model in Telework. Procedia - Social and Behavioral Sciences 229, 33–41. https://doi.org/10.1016/j.sbspro.2016.07.111

Woon, I., Tan, G.-W., Low, R., 2005. A protection motivation theory approach to home wireless security. ICIS 2005 proceedings 31.

World Economic Forum, 2018. Cyber Resilience Playbook for Public-Private Collaboration.

World Economic Forum, 2015. Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats.

Yildirim, Y.E., Akalp, G., Aytac, S., Bayram, N., 2011. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. International Journal of Information Management 31, 360–365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006

Zahadat, N., Blessner, P., Blackburn, T., Olson, B.A., 2015. BYOD security engineering: A framework and its analysis. Computers & Security 55, 81–99. https://doi.org/10.1016/j.cose.2015.06.011

Appendices

Appendix A: Survey instrument

A-1 Section 1: Demographic information

Please select your gender

☐ Male ☐ Female

What is your highest level of education?

☐ High school ☐ Vocational training (TAFE, VET) ☐ Diploma (Advance diploma, Associate degree)

☐ Bachelor's degree ☐ Master's degree ☐ Doctorate ☐ Other (please)

Please select your age

☐ 18 – 24 ☐ 25 – 34 ☐ 35 – 44 ☐ 45 – 55 ☐ 55 and over

What is your role in the organisation?

☐ Owner ☐ Administrative ☐ Technical

☐ Managerial ☐ Supervisory ☐ Consultant ☐ Other

What industry best categorises your organisation?

☐ Manufacturing

☐ Construction

☐ Finance and Insurance services

☐ Accommodation and food services

☐ Other

☐ Professional, Scientific and Technical services

☐ Rental, Hiring and Real Estate Services

☐ Health care and Social Assistance

☐ Education and Training

What is the size of your organisation? (number of employees)

☐ 0 – 4 ☐ 5 – 19 ☐ 20 – 199 ☐ 200 – 499 ☐ 500 – 999 ☐ greater than 1000

How many years have you been working for this organisation?

☐ 0 – 4 ☐ 5 – 9 ☐ 10 – 14 ☐ more than 15 years

The rest of the questions in this section refer to two policies in your organisation. The first is the information security policy. The second is the personal devices in the workplace (such as Bring Your Own Device (BYOD) policy).

Information security policies are formal written rules or procedures that apply to all individuals accessing and using the organisation's information technology assets and resources. The policies may include procedures such as using public Wi-Fi, social media use and sending confidential documents.

A **bring your own device (BYOD) policy** is a set of rules that employees should adhere to when using their own personally owned device (such as a personal laptop) to access the organisation's information assets when performing work tasks (e.g. accessing email, customer data, inventory data and sending documents).

Does your organisation have a written information security policy?

☐ Yes ☐ No ☐ I don't know

If you answered 'Yes', to the question above, to what extent are you aware of the contents of the information security policy in your organisation?	Completely aware	Moderately aware	Slightly aware	Neutral	Slightly unaware	Moderately unaware	Completely unaware

Does your organisation have a written policy on the use of personal devices (for example a BYOD policy)?

☐ Yes ☐ No ☐ I don't know

If you answered 'Yes', to the question above, to what extent are you aware of the details in the policy?	Completely aware	Moderately aware	Slightly aware	Neutral	Slightly unaware	Moderately unaware	Completely unaware

A-2 Section 2: General behaviour questions

Instructions: In this section, you are asked questions about your activities when working (from the office or another location) using your personal device (such as personal laptop).

For all questions in this section, please consider your organisation's policies (security policy and user device policy if your organisation has implemented them) when answering.

Please respond openly and honestly knowing that your answers are completely anonymous and confidential.

Please indicate the extent (on a 1 to 7 scale) to which you agree with the statements when working: (1 = strongly disagree; 2 = moderately disagree; 3 = slightly disagree; 4 = neither disagree nor agree; 5 = slightly agree; 6 = moderately agree; 7 = strongly agree).

CONSTRUCT	ITEMS
BEHAVIOUR (THOMPSON ET AL., 2017)	For my personal device, I have installed security software.
	For my personal device, I have recent backups.
	For my personal device, I have enabled automatic updating of my computer software.
	For my personal device, I use security software (anti-virus/anti malware).
	For my personal device, it is secured by a password.
ATTITUDE (IFINEDO, 2012; THOMPSON ET AL., 2017)	To me, complying with the requirements of my organisation's information security policy/measure is beneficial.
	To me, complying with the requirements of my organisation's information security policy/measure is important.

	To me, complying with the requirements of my organisation's information security policy/measure is useful.
	To me, complying with the requirements of my organisation's information security policy/measure is necessary.
	I follow my organisation's information security policy /measures.
INTENTION (AJZEN, 2002: IFINEDO, 2012)	I intend to comply with my organisations information security policy/measures.
	I want to comply with my organisations information security policy/measures.
	I expect to comply with my organisations information security policy/measures.
STRESS (MOORE, 2000; AYYAGARI ET AL., 2011; MAIER ET AL., 2015)	Complying with the requirements of information security policies/measures in my organisation stresses me out.
	Complying with the requirements of information security policies/measures of my organisation puts an additional workload on me.
	Complying with the requirements of the information security policies/measures in my organisation exceed my available mental resources.
	I feel drained from activities that require me to comply with my organisation's information security policies/measures.
	I feel tired from my activities regarding complying with my organisation's information security policies/measures.
	Complying with my organisation's information security policies/measures is a strain for me.
HABIT (VERPLANKEN AND ORBELL, 2003; VANCE ET AL., 2012)	Complying with information security policies/measures is something I do frequently.
	Complying with information security policies/measures is something I have no need to think about doing.
	Complying with information security policies/measures is something that's typically ''me.''
	Complying with information security policies/measures is something I have been doing for a long time.
	Complying with information security policies/measures is something I do automatically.
	Complying with information security policies/measures is something I do without having to consciously remember to do so.
	Complying with information security policies/measures is something that makes me feel weird if I do not do it.
	Complying with information security policies/measures is something I do without thinking.
	Complying with information security policies/measures is something that would require effort not to do.
	Complying with information security policies/measures is something that belongs to my (daily, weekly, monthly) routine.
	Complying with information security policies/measures is something I start doing before I realize I'm doing it. Complying with information security policies/measures is something I would find hard not to do.
SUBJECTIVE NORMS (IFINEDO, 2012; THOMPSON ET AL., 2017)	Friends who influence my behaviour would think that I should take measures to secure my personal devices.
	Significant others who are important to me would think that I should take measures to secure my personal devices.
	My peers would think that I should take security measures on my personal devices.
HARDINESS (BARTONE, 1991)	Most of my life gets spend doing things that are worthwhile. (cm)
	Working hard doesn't matter, since only the bosses profit by it. (r)(cm)
	By working hard, you can always achieve your goals. (cm)

	I am really look forward to my work. (cm)
	Thinking of yourself as a free person just leads to frustration. (r)(cm)
	Trying your best at work really pays off in the end. (cm)
	Lots of times, I don’t really know my own mind. (r)(cm)
	Most days, life is really interesting and exciting for me. (cm)
	It’s hard to imagine anyone getting excited about working. (r)(cm)
	Ordinary work is just too boring to be worth doing. (r)(cm)
	Planning ahead can help avoid most future problems. (co)
	No matter how hard I try, my efforts usually accomplish nothing. (r)(co)
	Most of what happens in life is just meant to be. (r)(co)
	When I make plans, I’m certain I can make them work. (co)
	If I am working on a difficult task, I know when to seek help. (co)
	Most of the time, people listen carefully to what I say. (co)
	My mistakes are usually very difficult to correct. (r)(co)
	Most good athletes and leaders are born, not made. (r)(co)
	I can’t do much to prevent it if someone wants to harm me. (r)(co)
	What happens to me tomorrow depends on what I do today. (co)
	The “tried and true” ways are always best. (r) (ch)
	I don’t like to make changes in my everyday schedule. (r)(ch)
	It’s exciting to learn something about myself. (ch)
	I won’t answer a question until I am really sure I understand it. (r)(ch)
	I like a lot of variety in my work. (ch)
	It bothers me when my daily routine gets interrupted. (r)(ch)
	I often wake up eager to take up my life wherever it left off. (ch)
	I respect rules because they guide me. (r)(ch)
	I like it when things are uncertain or unpredictable. (ch)
	Changes in routines are interesting to me. (ch)
PERCEIVED SEVERITY (VANCE ET AL., 2012)	An information security breach in my organisation would be a serious problem for me.
	If I would do what is described in the scenario, there would be serious information security problems for my organisation.
PERCEIVED VULNERABILITY (VANCE ET AL., 2012)	I could be subjected to an information security threat, if I would do what is described in the scenario.
	My organisation could be subjected to an information security threat if I did what is described in the scenario.
	An information security problem could occur if I did what is described in the scenario.
PERCEIVED REALISM (VANCE ET AL., 2012)	How realistic do you think the above scenario is?

All items where measured on a seven-point Likert; (r) reversed item; (cm) commitment; (co) control; (ch) challenge

A-3 Section 3: Scenarios

Instruction: In this section, a work scenario is presented. You will be asked to respond to the questions referring to how you would act when carrying out work tasks if you were in the same situation.

Scenario background information: You are working as an accountant in a small business with 15 employees. Your business specialises in accounting, finance, and taxation services. A new client needs to provide personal information such as bank details, driver's license or passport details that are stored in the company's database. This information is classified as confidential and restricted to very few employees. You have access to this confidential customer information.

Employees are advised to encrypt any confidential information before transmitting and also use a virtual private network (VPN) when working outside the office.

Scenario 1 Office Secured Wi-Fi

You are working in the office where there is a secure Wi-Fi connection. This allows you to use your personal laptop to access work emails and customer information.

You are preparing a presentation for a scheduled one-hour meeting with a new important client who will be arriving in a few minutes. Just before the client arrives you receive an email from your boss instructing you to prepare a confidential financial report and send it in the next 30 minutes for an urgent meeting he has with another client. Your boss is very strict and expects employees to act swiftly when dealing with clients. You recall that a few months ago, some employees were sanctioned for failing to complete their tasks in time.

You could quickly finish preparing the presentation before the client arrives, however, due to the tight deadline you are not able to complete the document encryption. Using your personal laptop, you access the financial information required, generate the report, which contains confidential customer information, and email the unencrypted document to your boss.

Scenario 2 Cafe Unsecured Wi-Fi

You are meeting with a new client in a café that has free public Wi-Fi. You connect using your personal laptop to the network to check your emails.

You are preparing a presentation for a scheduled one-hour meeting with a new important client who will be arriving in a few minutes. Just before the client arrives you receive an email from your boss instructing you to prepare a confidential financial report and send it in the next 30 minutes for an urgent meeting he has with another client. Your boss is very strict and expects employees to act swiftly when dealing with clients. You recall that a few months ago, some employees were sanctioned for failing to complete their tasks in time.

You could quickly finish preparing the presentation before the client arrives, however, due to the tight deadline you are not able to complete the document encryption. Using your personal laptop, you access the financial information required, generate the report, which contains confidential customer information, and email the unencrypted document to your boss.

Scenario 3 Office Secure Wi-Fi no urgency

You are working in the office where there is a secure Wi-Fi connection. This allows you to use your personal laptop to access work emails and customer information.

Since there is not a lot of work due today, you are preparing a presentation for a scheduled one-hour meeting with a new important client which will take place tomorrow. Using your personal laptop, you receive an email from your boss instructing you to prepare a confidential financial report and send it by tomorrow for a meeting he has with another client. Your boss is very strict and expects employees to act swiftly when dealing with clients. You recall that a few months ago, some employees were sanctioned for failing to complete their tasks in time.

You finish preparing for meeting with the client, and send the report to him as soon as possible, you do not use a Virtual Private Network (VPN) or encrypt the file.

Scenario 4 Café Unsecured Wi-Fi no urgency

You are working from a café that has free public Wi-Fi. You connect using your personal laptop to the network to check your emails.

Since there is not a lot of work due today, you are preparing a presentation for a scheduled one-hour meeting with a new important client which will take place tomorrow. You receive an email from your boss instructing you to prepare a confidential financial report and send it by tomorrow for a meeting he has with another client. Your boss is very strict and expects employees to act swiftly when dealing with clients. You recall that a few months ago, some employees were sanctioned for failing to complete their tasks in time.

You finish preparing the presentation for the client, and prepare the report for your boss, and send it to him as soon as possible, you do not use a Virtual Private Network (VPN) connection or encrypt the file.

Appendix B: Ethics Approval

B-1 Ethics Approval

---

ethics application (5201701166)

Irene Chen <i.chen@mq.edu.au> Tue, Dec 19, 2017 at 1:42 PM

To: Yvette Blount <yvette.blount@mq.edu.au>

Cc: Mauricio Marrone <mauricio.marrone@mq.edu.au>, "queen.aigbefo@students.mq.edu.au" <queen.aigbefo@students.mq.edu.au>, Nikola Balnave <nikki.balnave@mq.edu.au>, FBE Ethics <fbe-ethics@mq.edu.au>

Dear Dr Blount

Re application entitled: Understanding SME employees' risk behaviour when performing work task using BYOD from multiple work locations

Reference Number: 5201701166
The above application was reviewed by the Faculty of Business & Economics Human Research Ethics Sub Committee. Approval of the above application is granted, effective "19/12/2017". This email constitutes ethical approval only.

This research meets the requirements of the National Statement on Ethical Conduct in Human Research (2007). The National Statement is available at the following web site: http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/e72.pdf.

The following personnel are authorised to conduct this research:

Dr Yvette Blount

Dr Mauricio Marrone

Ms Queen Aigbefo

NB. STUDENTS: IT IS YOUR RESPONSIBILITY TO KEEP A COPY OF THIS APPROVAL EMAIL TO SUBMIT WITH YOUR THESIS.

Please note the following standard requirements of approval:

1. The approval of this project is conditional upon your continuing compliance with the National Statement on Ethical Conduct in Human Research (2007).

2. Approval will be for a period of five (5) years subject to the provision of annual reports.

Please retain a copy of this email as this is your official notification of ethics approval.

Yours sincerely,

Dr. Nikola Balnave
Chair, Faculty of Business and Economics Ethics Sub-Committee

Faculty of Business and Economics

Email: fbe-ethics@mq.edu.au

www.businessandeconomics.mq.edu.au/

B-2: Ethic amendment approval

From: Irene Chen on behalf of FBE Ethics
Sent: Monday, 26 February 2018 12:16 PM
To: Yvette Blount
Cc: FBE Ethics; Nikola Balnave
Subject: Ethics amendment (5201701166)

Dear Dr Blount

Re: Project entitled: Understanding SME employees' risk behaviour when performing work task using BYOD from multiple work locations

Reference No.: 5201701166

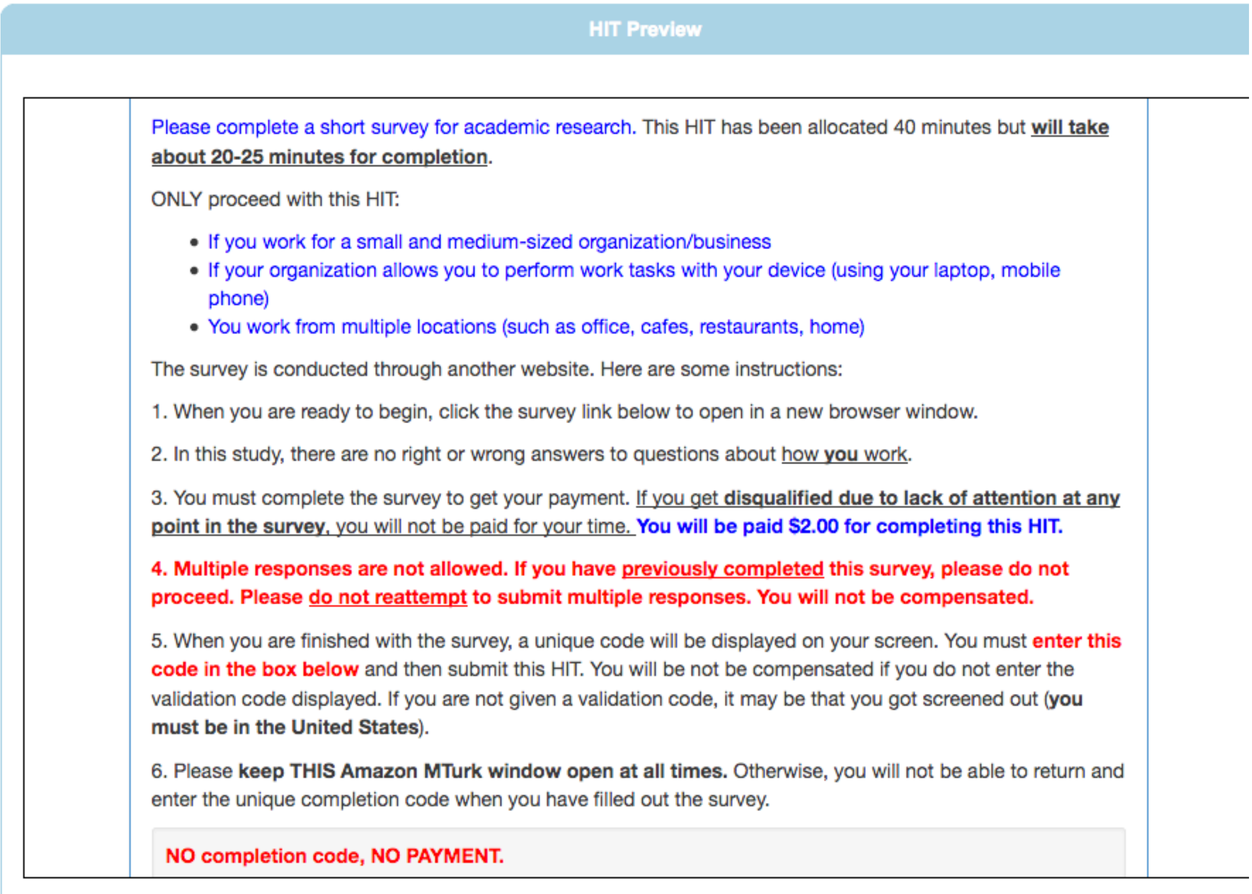
Thank you for your recent correspondence. The following amendments have been approved:

- Amendment to enable researchers collect data using a readily available platform called Amazon MTurk

If you have any questions or concerns please contact the FBE Ethics Secretariat on 9850 4826 or at the following email fbe-ethics@mq.edu.au

Yours sincerely,
Dr. Nikola Balnave

Appendix C: MTurk advert instructions



Please complete a short survey for academic research. This HIT has been allocated 40 minutes but **will take about 20-25 minutes for completion**.

ONLY proceed with this HIT:

- If you work for a small and medium-sized organization/business
- If your organization allows you to perform work tasks with your device (using your laptop, mobile phone)
- You work from multiple locations (such as office, cafes, restaurants, home)

The survey is conducted through another website. Here are some instructions:

1. When you are ready to begin, click the survey link below to open in a new browser window.

2. In this study, there are no right or wrong answers to questions about how **you** work.

3. You must complete the survey to get your payment. If you get **disqualified due to lack of attention at any point in the survey**, you will not be paid for your time. **You will be paid $2.00 for completing this HIT.**

4. Multiple responses are not allowed. If you have previously completed this survey, please do not proceed. Please do not reattempt to submit multiple responses. You will not be compensated.

5. When you are finished with the survey, a unique code will be displayed on your screen. You must **enter this code in the box below** and then submit this HIT. You will be not be compensated if you do not enter the validation code displayed. If you are not given a validation code, it may be that you got screened out (**you must be in the United States**).

6. Please **keep THIS Amazon MTurk window open at all times.** Otherwise, you will not be able to return and enter the unique completion code when you have filled out the survey.

NO completion code, NO PAYMENT.