2020

Understanding Contextual Factors of Bring Your Own Device and Employee Information Security Behaviors from the Work-Life Domain Perspective

Mohamed Alaskar
University of Wollongong in Dubai

Understanding Contextual Factors of Bring Your Own Device and Employee Information Security Behaviors from the Work-Life Domain Perspective

A thesis submitted in partial fulfilment of the requirements for the award of the degree of

Doctor of Philosophy

UNIVERSITY OF WOLLONGONG IN DUBAI

by

Mohamed Alaskar

Supervisor

Dr. Kathy Ning Shen

University of Wollongong in Dubai

Dubai, United Arab Emirates

Co-Supervisor

Professor Douglas R. Vogel

Harbin Institute of Technology

Harbin, China

2020

Faculty of Business

CERTIFICATION

I, Mohamed Alaskar, declare that this thesis, submitted in partial fulfillment of the requirements for the award of Doctor of Philosophy, in the Faculty of Business and Management, University of Wollongong in Dubai, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualifications at any other academic institution.

_____

August 2020.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BYOD:	Bring Your Own Device
DT:	Deterrence Theory
ICT:	Information and Communication Technology
IS:	Information Security
LWD:	Work-Life Domain
PBC:	Perceived Behavioral Control
PDA:	Personal Digital Assistant
PMT:	Protection Motivation Theory
PTS:	Perceived Threat Severity
PTV:	Perceived Threat Vulnerability
RC:	Response Cost
RE:	Response Efficacy
RWD:	Rewards
SE:	Self-Efficacy
TRA:	Theory of Reasoned Action
WFH:	Work from Home
WFX:	Work from Anywhere

ABSTRACT

Bring Your Own Device (BYOD) is no longer the exception, but rather the norm. Most prior research on employees' compliance with organizational security policies has been primarily conducted with the assumption that work takes place in a specified workplace, not remotely. However, due to advances in technology, almost every employee brings his or her own device(s) to work. Further, particularly as a result of the 2020 Covid-19 pandemic, remote working has become very popular, with many employees using their own devices for work-related activities. BYOD brings new challenges in ensuring employees' compliance with information security rules and policies by creating a gray area between the work and life domains as it diminishes the boundaries that separate them and thus affects employees' perception of them. As yet, little is known about how BYOD changes individuals' perception of work-life domains and how such perception may subsequently affect their compliance behavior.

Building on prior research on information security behaviors and work-life domain management, this thesis investigates the possible effects of BYOD on employees' compliance behavior through the changes it brings about in their work-life domain perspective. It extends existing border theory by identifying and empirically validating new border marking factors—namely, device ownership and data sensitivity—in employees' interpretation of their work and life domains. Subsequently, protection motivation theory, a theory widely used in explaining employees' compliance behavior, was used to examine why and how the perception of work-life domains is relevant and necessary to consider in examining employees' intention to comply with information security policies.

The thesis proposes two research models (i.e. re-conceptualization of border theory based on BYOD contextual factors and the impact of employees' perception of which domain they are in (i.e., life domain or work domain) and the impact of on their intention to comply with information security policy). The two models were tested by developing BYOD usage scenarios based on BYOD contextual factors that drove the survey design used for the data collection. A panel was used to collect the data, which resulted in 3035 usable responses. Multiple regression analysis was used to analyze the collected data. Based on the result of the analysis, the proposed BYOD contextual factors, including device ownership, employees' location, time of activity, and activity type, were shown to have a significant impact on employees' perception of work-life domain. Also, the impact of variables from the protection

motivation theory, except for perceived response-efficacy, changed based on employees' perception of whether they were in the life or work domain. When employees perceived themselves to be in the life domain, only perceived self-efficacy and perceived response efficacy were found to have a significant effect. When employees perceived themselves to be in the work domain, perceived threat severity, perceived threat vulnerability, perceived self-efficacy, and perceived response efficacy were found to have significant effects. However, in the gray areas, when employees were unable to differentiate between the two domains, all of the protection motivation theory variables were found to have a significant effect (albeit rewards and perceived self-efficacy had a negative rather than positive effect).

The results of the thesis offer several theoretical contributions. First, a new BYOD contextual factors framework has been developed and empirically validated. The framework provides a new perspective to re-examine different employee behaviors. Second, the thesis contributes to the work-life domain literature by introducing BYOD and its relationship to employees' sense-making of being in the life or work domain. It also sheds light on a new aspect that affects employees' information security behaviors, i.e., their perception of being in the work or life domain. This was presented by showing how one of the most used theories in information security behavior studies, protection motivation theory, was affected by employees' perception of which domain they were in. The findings of this thesis have significant practical implications by providing organizations and practitioners with guidance on how to design information security policies to be more effective.

ACKNOWLEDGMENTS

Everything I am today is a blessing from Allah.

Allah blessed me to have a father and a mother that raised me with kindness and guided me with values. They provided me with everything to be the man I am today. They love me unconditionally and have always been there for me. I am always and forever in their debt. I will always love you and be your son.

Allah blessed me to be born in the best country anyone can ask for, the United Arab Emirates. A peaceful multicultural country led by visionary leaders that believe in us, invest in us, and provide us with everything a person can ask for. I can never pay my country back, but I will always work in any aspect that contributes to its growth.

Allah blessed me with many people that I can genuinely call lifelong friends. They have been with me in my joyful times and in my time of need. To Mohamed Al Marzooqi, Mohamed Al Ali, Yasser Ashmawy, Mohamed Abdulla, Saeed Al Mansoori, Mansoor Al Marzooqi, Rami Yazbek, and Ali Al Ketbi, I'm grateful to have you in my life.

Allah blessed me with the best supervisor I could ever ask for, Dr. Kathy Ning Shen. She supported me through my PhD journey. She was patient with me and pulled me back every time I lost track. She kept pushing me to get my thesis completed. She is the main reason that I reached the final stage of my PhD and completed this thesis. I cannot express enough how thankful I am to you.

Allah blessed me with a loving family, brothers, sisters, nephews, nieces, uncles, aunts, extended family, supervisors, teachers, mentors, friends, and colleagues. I would like to thank you all for being there, tolerating my shortcomings, and supporting me wherever you could. My life would not be the same without you.

Thank you.

CHAPTER ONE: INTRODUCTION AND MOTIVATION

This chapter provides an overview of the overall purpose and scope of this thesis. It starts by presenting the criticality of information security for organizations in the information age. Next, it illustrates how the human factor (i.e., employees), being the weakest link in information security, plays an essential role in securing organizations' information assets. It then discusses how the adoption of the Bring Your Own Device (BYOD) concept posits a new threat to information security, primarily because of its capacity to affect employees' sense-making of being in the life domain or work domain which, in turn, affects their information security-related behaviors. The research question and objectives of investigating this topic are then put forward. Finally, the last section of this chapter provides an overview of the structure of the thesis.

1.1 Background

Today's high dependence on technology in the day-to-day operations of many organizations worldwide means that information security is an ongoing concern. The use of technology—although it has introduced many benefits—has also introduced many information security threats that can have negative impacts on organizations. According to the Ponemon Institute (2017a), in 2017, there was an annual average of 130 security breaches per organization while a similar report by Bissell et al. (2019) shows an average of 145 breaches. The average cost of cyber-attacks reached $11.7 million annually in 2017, up from $7.2 million in 2013; in one case a single attack was estimated to have caused US$77.1 million of damage (Ponemon Institute, 2017a). The average cost of cyber-attacks increased by 12% in 2019 to $13 million (Bissell et al., 2019). Based on a survey of 4,644 organizations, 83% reported an average cost per attack of $380,000 (Bissell et al., 2020). Accordingly, organizations spend a considerable amount of resources on protecting their information: $101,544 million in 2017 which was forecast to increase to $124,116 million in 2019 (Moore and Keen, 2018).

One of the primary threats facing organizations' information security comes from their employees, referred to in the literature as security's weakest link (e.g., Sasse et al., 2001; Bulgurcu et al., 2010a; Dong et al., 2010; Hu et al., 2011; Caldwell, 2012; Johnston et al., 2016). Security breaches by employees—whether intentional or unintentional, malicious or non-malicious—can cause harm to organizational information security (Jouini et al., 2014).

According to Verizon (2020), internal actors accounted for 30% of breaches in information security, 8% of which were due to employee misuse (i.e., not following information security policy (but without a malicious intent) such as not logging off from an unattended computer). On average, it takes an organization 50 days to resolve a malicious insider's attack, and it is the most expensive form of attack to resolve, with an average cost of $173,516 per attack (Ponemon Institute, 2017a). Because of this threat, organizations invest resources in implementing information security policies which aim to direct their employees to behave in a manner that ensures the protection of their information assets. In many cases, the absence of such policies results in information security incidents. For instance, a report by Maple and Phillips (2010) shows that almost all case studies that did not have an information security policy in place suffered from security breaches. Furthermore, even in cases where organizations had an information security policy, they were not confident that their employees were adhering to it (Ponemon Institute, 2010).

The threat posed by employees as the weakest link has led many researchers to investigate their behaviors when it comes to information security and their compliance with information security policy (e.g., Ng et al., 2009; Zhang et al., 2009a; Ifinedo, 2014). Such endeavors aimed to determine the factors that drive employees' information security behaviors to better guide the process of designing information security intervention programs that aim to change employees' behaviors (e.g., Bulgurcu et al., 2010a; Ifinedo, 2012; Johnston et al., 2015). The success of such programs will have a significant impact on employees' behaviors and, as a result, improve security practices in their organizations (e.g., Bulgurcu et al., 2010a; Ifinedo, 2012; Johnston et al., 2015).

With the never-ending innovation in the Information and Communication Technology (ICT) field, new opportunities are constantly introduced to organizations, many of which impact their information security. Among these new opportunities, ICT has enabled organizations to take on board more flexible working arrangements, allowing employees to work from any place and at any time (Park and Jex, 2011), and both organizations and employees have adopted such strategies to exploit the expected benefits. For example, some employees telecommute to work to eliminate wasted time (and money) spent on long commutes. At the same time, some organizations expect cost savings by adopting these more flexible working arrangement strategies (Lewis and Cooper, 2005).

One of the strategies used by organizations to enable their employees to work from any place and at any time is Bring Your Own Device (BYOD). BYOD refers to the practice whereby an organization permits its employees to use their personally-owned devices (e.g., smartphones, tablets, and laptops) to perform work-related tasks inside or outside of the workplace. Employees expect their personally-owned devices to have access to and be integrated with the organizations' information systems (e.g., network, applications, and information) (e.g., Disterer and Kleiner, 2013; Tokuyoshi, 2013; Crossler et al., 2014; Garba et al., 2015). A 2013 survey of thousands of employees showed that the majority of them were using their own devices for work (Bradley et al., 2012); even when an organization expressly forbade the use of personally-owned devices to do work tasks, employees still used their own devices (Garba et al., 2017). A more recent study of more than 2000 organizations showed that 45% of employees were using personally-owned devices for work activities (Vaidya, 2018). With this increasing dependence on mobile devices, organizations expect their employees to continue working after office hours, even from home (Disterer and Kleiner, 2013) while, on the other hand, employees bring personal activities to their work environments (e.g., social media, personal email) (Disterer and Kleiner, 2013; Dang and Pittayachawan, 2015).

The implications of BYOD have intrigued researchers as well as practitioners. Some prior research has revealed positive impacts in terms of employee satisfaction, usability, mobility, efficiency, productivity, and lowering of operational costs for organizations (e.g., Tokuyoshi, 2013; Crossler et al., 2014; Willis, 2014; Garba et al., 2015). Giving employees the freedom to use their own devices is expected to increase job satisfaction (e.g., Thomson, 2012; Disterer and Kleiner, 2013; Moyer, 2013; Willis, 2014; Garba et al., 2015). Moreover, it is argued that employees have a better understanding of the usability requirements (e.g., device features, applications) necessary to perform their day-to-day work-related tasks which will be reflected in the device they bring to work (Tokuyoshi, 2013). By applying BYOD and integrating employees' devices with organizational information systems, employees have more freedom to work at any time and from any place (Disterer and Kleiner, 2013)—and more satisfied employees equipped with usable and mobile devices can also increase efficiency (e.g., Disterer and Kleiner, 2013; Crossler et al., 2014; Garba et al., 2015). Finally, employees are responsible for maintaining their own devices, leading to reductions in the cost of organizational operations (Dang and Pittayachawan, 2015; Garba et al., 2015).

While many prior studies have discussed the positive implications of BYOD (e.g., Crossler et al., 2014; Dang and Pittayachawan, 2015; Garba et al., 2015), the phenomenon also poses several challenges, specifically to organizational information security (Disterer and Kleiner, 2013). The adoption of BYOD without proper consideration of the information security implications means that organizations risk data loss (Garba et al., 2017) through, for example, unauthorized data sharing, issues with access controls, device management challenges, hacking, device loss or theft, malware, and security controls on apps used by users (Garba et al., 2015; Garba et al., 2017). Even in those organizations that have a better understanding of BYOD risks, the risks are often not recognized by the employees nor reflected in the security guidelines (Doargajudhur and Dell, 2019). The information security risks associated with BYOD have led some to refer to it as "Bring Your Own Danger"(Doargajudhur and Dell, 2019).

1.2 Research Gaps and Motivation

Traditionally, information security policies—together with awareness campaigns, training, incentive schemes, and disciplinary procedures—are designed to regulate employees' behaviors, make effective changes to it, ensure compliance with the policies, and ultimately, protect the organization's information assets (Bulgurcu et al., 2010a). However, the vast majority of these policies are designed to regulate employees' behaviors when they are using company-owned devices (Garba et al., 2017). A 2018 survey of more than 2000 organizations, showed that while 45% of employees regularly used personally-owned devices for work, only 19% of these organizations had a policy on the usage of personally-owned devices for work-related activities (Vaidya, 2018). Even those organizations that had a BYOD specific policy in place treated personally-owned devices the same as company-owned devices (Garba et al., 2017).

Furthermore, there is a dearth of studies on the subject of BYOD challenges and effective BYOD management (Garba et al., 2017). The majority of information security studies have focused on behaviors related to the usage of company-owned devices and organizational settings (e.g., Straub Jr, 1990; Gopal and Sanders, 1997; Bulgurcu et al., 2010a; Palanisamy et al., 2020b).

The vast majority of prior studies focused on organizational settings and testing the application of different theories. Many theories have been used to explain information security-related

behavior including the theory of reasoned action (TRA) (e.g., Bulgurcu et al., 2010a; Ifinedo, 2012), protection motivation theory (PMT) (e.g., Workman et al., 2008; Johnston and Warkentin, 2010), deterrence theory (DT) (e.g., Straub Jr, 1990; Gopal and Sanders, 1997), and rational choice theory (RCT) (e.g., Hu et al., 2011; Han et al., 2017), among others. These studies have provided many insights and several contributions to better understand the different variables influencing information security behaviors. However, only a few studies have been identified that examine information security behaviors outside of the work environment and just two on BYOD (Crossler et al., 2014; Dang and Pittayachawan, 2015).

The two BYOD studies have started to examine some of the contextual factors relevant to BYOD. For instance, Dang-Pham and Pittayachawan (2015) examined the spatial contextual factor by studying the effect of non-work activities at home and in the workplace when employees use their own devices. They used an extended version of the protection motivation theory and found that the spatial contextual factor impacts the PMT variables' effect on information security behavior intent. Crossler et al. (2014) examined the effect of psychological factors related to BYOD and showed that the sensitivity of data affects PMT variables that affect employees' behaviors when using their own devices. The unique contextual factors related to BYOD were not sufficiently discussed in these papers—only some of the factors were considered and investigated. There was no evidence of establishing a comprehensive framework capturing the complexity of BYOD and defining related contextual factors and their effects on information security-related behaviors.

Some of the contextual factors in the BYOD studies have also been examined in the work-life domain literature. These contextual factors, in addition to others that have not been examined in BYOD studies, have been shown to blur the boundaries between the work and life domains (e.g., Chesley, 2005; Leung, 2011). These included physical, temporal, behavioral, social, and psychological factors (e.g., Ashforth et al., 2000; Clark, 2000; Olson-Buchanan and Boswell, 2006; Park and Jex, 2011; Fonner and Stache, 2012). Further, the effect of work-life domain management on employees and organizational behaviors, and firm productivity has been discussed and presented in several studies (e.g., Konrad and Mangel, 2000; Lambert, 2000; Bragger et al., 2005; Muse et al., 2008). Employees of organizations that supported them to better balance their work and life demands exhibited more positive attitudes and behaviors (Muse et al., 2008) which were reflected in their overall task and contextual performance (Muse et al., 2008). Similarly, organizational support for employees' work-life balance have been

shown to positively affect employee efforts to improve their organization (Lambert, 2000). Working in the office had a different effect from working from home on aspects such as job performance, motivation, retention, and workload success (Hill et al., 2003). Also, being in the work environment and atmosphere has been shown to have a different effect on employee concentration and decision-making from being in a non-work environment and atmosphere (Burmeister et al., 2018).

As discussed above, BYOD has similar contextual factors to those identified in the work-life domain literature (e.g., Ashforth et al., 2000; Clark, 2000; Olson-Buchanan and Boswell, 2006; Park and Jex, 2011; Fonner and Stache, 2012; Crossler et al., 2014; Dang and Pittayachawan, 2015) which have been shown to blur the boundaries of the work and life domains (e.g., Chesley, 2005; Leung, 2011). Therefore, this thesis argues that BYOD also blurs the boundaries between the work and life domains, affecting employees' perception of which domain they are in. Further, the perception of which domain they are in has been shown to influence employees' behaviors (e.g., Hill et al., 2003; Burmeister et al., 2018). Consequently, this thesis argues that employees' information security behaviors will be affected by their perception of whether they are in the work or the life domain. Employees will develop their own interpretation of BYOD—concerning the work-life domain—and adopt respective rules and norms (Li and Siponen, 2011; Dang et al., 2013). For instance, an employee performing work-related tasks in the workplace using his/her own device will have more awareness of his/her behaviors to avoid breaking information security policies and rules. However, an employee using the same device at home and performing non-work activities is extremely unlikely to consider information security policies due to the more relaxed environment he or she is experiencing. Thus, the complexity of BYOD contextual factors must first be understood; only then can the implications of BYOD on information security and related policy-making practices be investigated.

1.3 Research Question

As stated in the previous section, today, many employees use their own devices to do work-related activities (e.g., Garba et al., 2017; Vaidya, 2018). The use of employee-owned devices provides them with the flexibility to do their work at any place, any time (e.g., Tokuyoshi, 2013; Crossler et al., 2014; Willis, 2014; Garba et al., 2015). However, this poses new challenges to information security (Garba et al., 2015) as traditional information security policy is designed to address the requirements when employees are using company-owned devices,

not their personal devices (Garba et al., 2017). To address this gap, this thesis aims to expand on existing research by studying the contextual uniqueness of BYOD. This will be examined based on the results of prior studies related to 1) ICT effects on the management of work and life domains (e.g., Chesley, 2005; Hubers et al., 2011; Leung, 2011), and 2) behavior changes based on individual perceptions of being in the life domain or in the work domain (e.g., Hill et al., 2003; Burmeister et al., 2018). Therefore, this thesis intends to answer the following research question:

What BYOD contextual factors affect employees' perception of being in the life or work domain and subsequent compliance with information security policies?

Primarily, this thesis seeks to achieve the following objectives:

- To develop a comprehensive understanding of what BYOD contextual factors affect employees' perceptions of being in the work domain or life domain.
- To examine how employees' perceptions of being in the work or life domain affect their compliance with the information security policy.
- To empirically validate the research model.

1.4 Research Significance and Expected Contributions

By acknowledging the complexity and uniqueness of BYOD, this thesis aims to develop a comprehensive BYOD contextual factors framework and validate it empirically. The framework provides a fresh perspective on and an opportunity to re-examine the usability of existing theories in explaining BYOD-related information security behaviors. The framework will also enable researchers to investigate other types of employee behavior and cognitive processes (such as job performance, knowledge sharing, and decision making) from a new angle.

In addition, and based on border theory, this thesis will test the effect BYOD contextual factors have on employees' perception of whether they are in the work domain or the life domain. Although the majority of the literature reviewed in this thesis showed the impact that ICT has on employees' work-life domain management, no studies specifically on BYOD and the work-life domain were identified. More specifically, this thesis will examine how the actual ownership of the device can affect employees' perception of which work domain they are

inhabiting. Device ownership is a new addition to the list of factors in the work-life domain literature when it comes to examining work-life boundary management.

Further, employees' information security behaviors will be studied from a new perspective that has not received much attention in the current literature. The thesis acknowledges that due to the current flexibility enabled by technology, more specifically, the usage of BYOD, information security extends beyond the work environment boundary. It also recognizes that people behave differently depending on whether they perceive they are in a work environment or non-work environment. Accordingly, it studies the effect that employees' perception of which domain they are in—work or life—has on their information security behaviors. More specifically, the thesis will test how this perception affects one of the most widely-used theories in information security literature, protection motivation theory.

Practically, the thesis will address the current gap that exists in information security policies that focus mostly on the work environment and company-owned devices. These policies are not sufficient to successfully implement information security in an always-online age when employees are empowered to perform any activity, in any place, on any device, and at any time. Accordingly, this thesis will guide organizations and practitioners to develop information security policies that recognize the real world and employees' practices. These policies need to ensure that they address the usage of any device (whether owned by employees or by the organization), from any place (in the office or at home), at any time (whether during working hours or outside working hours), and while performing any activities (personal or work-related). Such contextual aspects need to be reflected in the policy statements whose drafting may make use of the results of this thesis and future studies that expand on it.

The results of this thesis will also guide information security behavioral change programs which aim to enhance awareness and provide training to employees to shape their behaviors to those that are compliant with information security policies. The results of this study will provide these programs with areas that can be used as key messages that can effectively trigger behavioral changes. Such messages will address the contextual factors and also the essential aspects that trigger employees' intention to comply with information security policy. This study shows the importance of including BYOD contextual factors as protection motivation variables when designing these programs.

1.5 Thesis Overview

The remainder of this proposal is set out as follows: in Chapter 2, the literature review will consider the aspects covered in extant information security studies, specifically, the studies concerning information security policy compliancy behaviors. This chapter will also identify the different theories that have been used in information security literature and BYOD within the information security field, and identify and discuss the theoretical gaps. In Chapter 3, the research models will be presented along with their supporting rationale. Chapter 4 will detail the research design and methods used to test the proposed models. Chapter 5 will present the result of testing the research models, and Chapter 6 will discuss these results and the theoretical contributions and practical contributions. Finally, Chapter 7 will summarize the research and its outcomes.

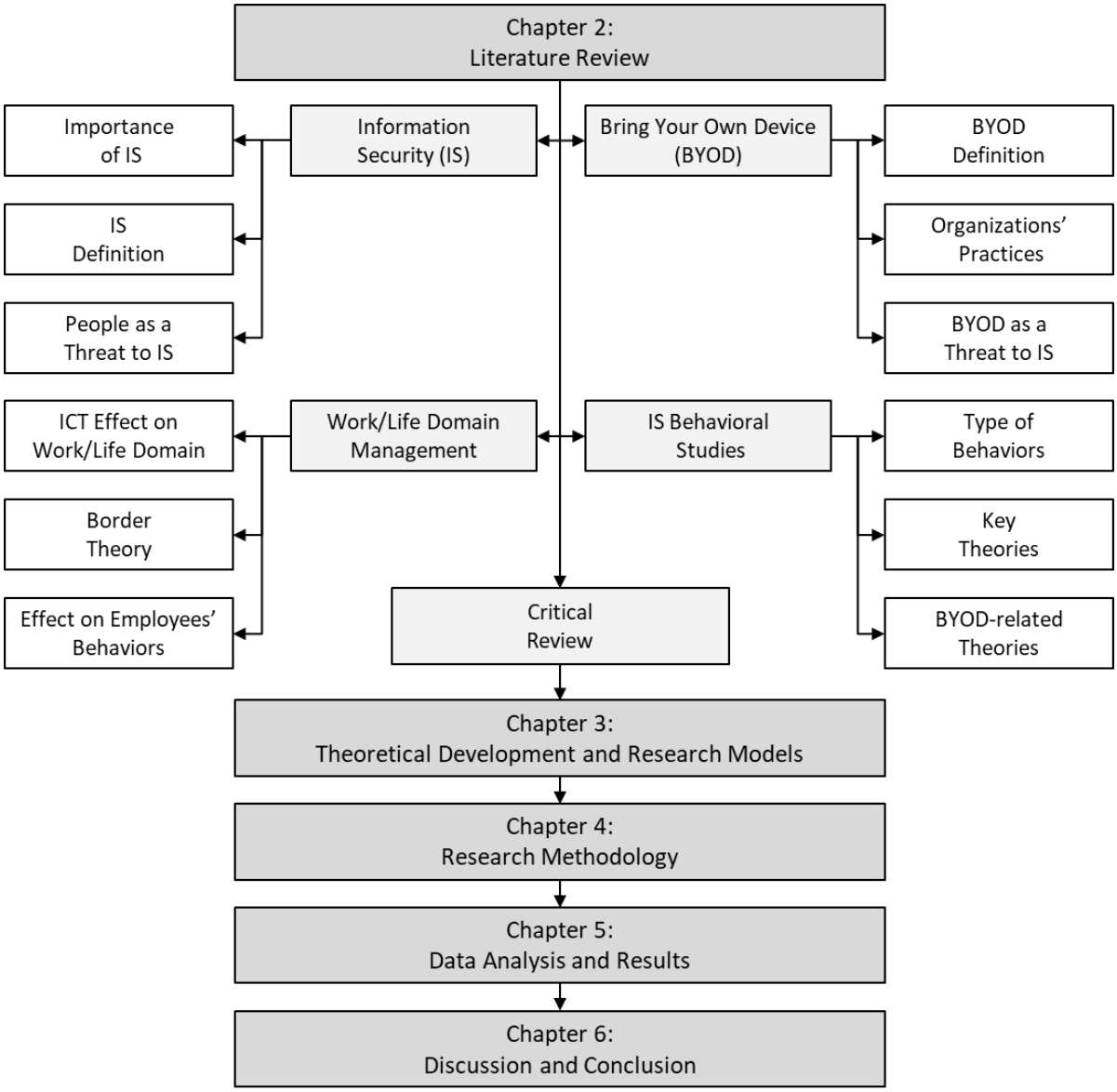


FIGURE 1: THESIS STRUCTURE

CHAPTER TWO: LITERATURE REVIEW

The literature review starts by providing an overview of information security, including its definition and the importance of employees' compliance with information security policy. It then provides a definition and overview of Bring Your Own Device (BYOD), and discusses how BYOD is becoming the norm. After that, the effects of BYOD on information security and current research gaps are presented. Further, an overview of the relations between BYOD and work-life domain management is given, showing how the literature of work-life domain management has discussed this phenomenon. Following that, the literature review provides a deep dive into the current studies investigating employees' information security-related behaviors to provide an understanding of the type of behaviors that have been examined and the key theories used. Finally, the conclusion connects the different studies from information security literature, work-life domain management literature, and BYOD literature to present and discuss the research gaps.

2.1 Information Security Overview

This section will aim to illustrate why information security is so critical in today's technologically advanced society. It will also define information security within this thesis's context based on the different definitions provided in the literature and used in practice. It will also discuss the different types of studies in the field of information security. Finally, this section will emphasize the importance of the human factor in the information security domain to ensure the protection of organization information assets.

2.1.1 Importance of Information Security

Information security is becoming one of the biggest concerns for organizations and is a top priority for around 74% of top management in different organizations (Vaidya, 2018). The importance of information security is driven by the ever-increasing number of security breaches. For example, the Ponemon Institute (2012) surveyed 56 organizations and found that they had encountered an average of 102 successful attacks per week; with a success rate of 1.8%, this means that each organization was suffering over 5000 attacks every week. By 2017, the average number of security breaches per company was increasing by 27.4% annually and had reached an average of 130 security breaches per company (Ponemon Institute, 2017a). In addition, Verizon (2012) reported that in 2011 around 174 million records had been compromised among the 90 organizations that it investigated. In the United States alone,

298,766,788 records were breached in 2012 (Privacy Rights Clearinghouse, 2012), increasing to 1,369,452,404 in 2018 (Privacy Rights Clearinghouse, 2018). In 2017, the global average for breached records was 24,089 records per company (Ponemon Institute, 2017b). Many other reports (e.g., Richardson, 2011; Ponemon Institute, 2013; Vaidya, 2018; Symantec, 2019) also illustrate different numbers of information security incidents that have occurred in different organizations.

These information security breaches and incidents place enormous burdens on organizations. The cost of security breaches has reached up to $5.4 million in some cases (Ponemon Institute, 2013), and each security attack costs organizations an average of $591,780 (Ponemon Institute, 2012). A survey by Potter and Waterfall (2012) of 447 organizations in the United Kingdom showed that the average loss due to information security breaches for small businesses was between £15,000 to £30,000. In contrast, the average loss for large organizations was between £110,000 and £250,000. Moreover, a 2012 Ponemon Institute survey of 56 organizations showed that the average cost resulting from cyber-crime was $8.9 million in 2012, with a minimum cost of $1.4 million and a maximum of $46 million. The average annual cost of cyber-crime increased to $11.7 million in 2017 (Ponemon Institute, 2017a).

As a result, organizations devote a great deal of their resources to implementing security countermeasures. *Infosecurity Magazine* (2012) reported that, globally, information security expenditures reached $55 billion in 2015. This figure increased to $101 billion in 2017 and was projected to increase further to $124 billion in 2019 (Moore and Keen, 2018).

2.1.2 Information Security Definition

Although the field of information security has gained a great deal of attention, the term has been interpreted in different ways in the literature. Drawing on Zhao and Lu (2007), Wang et al. (2010 p.65) defined information security as “the protection of information and information systems against unauthorized access or modification of information”, going on to add additional requirements for the protection of information and information systems against unauthorized usage, disruption, disclosure, and/or destruction. The scope of these two definitions encompasses both IT security (i.e., information systems security) and non-IT information security (e.g., physical security and human resources security). This means that all information within organizations is within the scope of information security, regardless of the type of medium. Consequently, information security is a bigger umbrella that encompasses information systems security.

However, the term ‘information systems security’ is also used in the literature (e.g., Smith and Jamieson, 2006; Vance et al., 2013) and has been defined as “the protection of information systems against unauthorized access to or modification of information whether in storage, processing, or transit, and against denial of service to authorized users, including those measures necessary to detect, document, and counter such threats” (NSTISSC 1999, p.4, cited in Smith and Jamieson, 2006 p.25). Examining this definition in the context of the previous two, it is clear that while this definition focuses only on the information systems protection aspect of information security, it elaborates more on the scope of the protection. Nevertheless, as stated earlier, information systems security is a subset of information security.

The International Organization for Standardization’s (ISO) definition of information security as “preservation of confidentiality, integrity, and availability of information” (ISO, 2009 p.3) is widely used in the practical world because many organizations have adopted the ISO/IEC 27000-series. However, for the sake of this study, the definition provided by the National Institute of Standards and Technology (NIST) will be used: “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (A) integrity, (B) confidentiality, and (C) availability” (National Institute of Standards and Technology (NIST), 2003 p.15). This definition encompasses all of the previous definitions while maintaining the broader scope of information security which covers all of the information that resides in the organization, whether in physical or electronic form.

2.1.3 Studies in the Information Security Field

The business world is not the only place that information security has gained importance; researchers also have shown interest, resulting in a large amount of literature focusing on different aspects of information security. Generally, prior research on information security has been conducted by two different streams of inquiry, focusing on either the implementation of information security or human factors. The former covers different topics that affect the success of information security implementation. For example, many researchers have focused on defining factors that positively or negatively affect the success of information security implementation (e.g., McFadzean et al., 2007; Dunkerley and Tejay, 2010; Smith, 2010; Hall et al., 2011) while others have focused on technical areas of information security (e.g., Bernardeschi et al., 2002; Jali et al., 2010; Zissis and Lekkas, 2011). Researchers have also studied information security awareness and training delivery methods and techniques (e.g.,

Kruger et al., 2010; Puhakainen and Siponen, 2010; Hagen et al., 2011). The second stream focuses mainly on the human effect on the information security ecosystem. For example, researchers have investigated factors leading individuals to commit security breaches (e.g., Shropshire, 2009; Garrison and Ncube, 2011) and individual behaviors, specifically behaviors related to information security policy compliance (e.g., Myyry et al., 2009; Bulgurcu et al., 2010a; Johnston and Warkentin, 2010; Siponen and Vance, 2010; Ifinedo, 2012). In this study, the focus will be on human factors to examine the impact of BYOD on information security.

2.1.4 Humans as the Key Threat to Information Security

A key factor that plays a considerable role in the success or failure of information security is the human factor (Johnston et al., 2016), also referred to as the weakest link in information security (e.g., Bulgurcu et al., 2010a; Dong et al., 2010; Caldwell, 2012). When it comes to organizations, employees represent this human factor and their behaviors affect information security within their organizations. Whether these behaviors cause harm intentionally or unintentionally, they remain critical. The data loss statistics found on the Datalossdb Open Security Foundation (2013) website show that around 24% of the total data loss incidents identified in 2012 were caused by insiders (i.e., employees) whether accidentally or maliciously. In addition, the survey by Potter and Waterfall (2012) revealed that employees are responsible for 42% of information security breaches in large organizations. Similarly, in 2012, in the United States alone, over 10 million records were reported to have been breached, with employees being the primary root cause, and this had increased to over 750 million in 2018 (Privacy Rights Clearinghouse, 2018). On the same topic, in 2013 the Ponemon Institute reported that the human factor accounted for 35% of data breaches globally. A similar figure was reported in 2017, where 28% of data breaches' root causes were associated with human error and negligence, while 47% were associated with malicious insider or criminal attacks (Ponemon Institute, 2017b). Similarly, Verizon (2019) reported that of 41,686 security incidents in 86 countries worldwide, internal actors were behind 34% of such incidents, 13% of which were due to misuse by authorized users. The cost of such breaches has been reported to be an average of $3.62 million (Ponemon Institute, 2017b).

Because of the impact employees have on information security, organizations develop and implement information security policies as one of the countermeasures to respond to the risks posed by employees' behaviors. Information security policy has been defined as a "statement of the roles and responsibilities of the employees to safeguard the information and technology

resources of their organizations" (Bulgurcu et al., 2010a pp.526-527). A report by Maple and Phillips (2010) found that every organization they studied which did not have an information security policy in place had suffered information security breaches. One can conclude from this that the absence of an information security policy is correlated with an organization's being at risk of information security breaches.

Although many organizations develop and implement information security policies, ensuring employees' compliance remains a challenge. A survey by Potter and Waterfall (2012) covering 447 UK organizations shows that 95% of large organizations have an information security policy in place but also reported that about 75% of organizations believe that their staff members have a poor understating of it. Similarly, Verizon (2012) reports 83% of large organizations have an information security policy in place; however a survey of 728 practitioners based in the United States shows that only a third (32%) were confident that their organization's information security policy is complied with. In contrast, around 68% of the respondents were not (Ponemon Institute, 2010).

Because of employees' noncompliance with information security policies, many researchers have been motivated to study the factors that influence this behavior. Such research has taken different approaches and proposed various explanations for employees' behaviors (e.g., Pahnila et al., 2007b; D'Arcy and Hovav, 2009; Herath and Rao, 2009a; Bulgurcu et al., 2010a; Hu et al., 2011; Son, 2011; Chen, 2012; Barlow et al., 2013; Crossler et al., 2014; Dang and Pittayachawan, 2015). The results of these studies have shed light on many factors such as self-efficacy (e.g., Bulgurcu et al., 2010a; Ifinedo, 2012; Johnston et al., 2015), response efficacy (e.g., Herath and Rao, 2009a; Ifinedo, 2012; Pahnila et al., 2013), attitude (e.g., Bélanger et al., 2017), injunctive norms (e.g., Hu et al., 2012; Al-Omari et al., 2013; Aurigemma and Mattson, 2017), and several other cognitive factors. Although the majority of these studies have focused on various cognitive factors, others have explored leadership style (e.g., Rocha Flores and Ekstedt, 2016; Amankwa et al., 2018), information security policy (e.g., Safa et al., 2015; Ahmad et al., 2019), information security Budget (Herath and Rao, 2009b), and information security awareness programs (e.g., Lee et al., 2004; D'Arcy and Hovav, 2007). However, the literature review shows that almost all of these studies have a focus on typical organizational settings. Only a few have looked into other aspects that might affect employee behaviors when they are not in a typical organizational setting—such as the concept of Bring Your Own Device (BYOD) and how it may disturb the normal typical organization setting (e.g., Crossler et al.,

2014; Dang and Pittayachawan, 2015; Garba et al., 2015). Their studies shed light on the potential of BYOD to have certain contextual factors that affect employees' compliance with information security policy. Accordingly, the literature review will discuss BYOD in more depth in the next section to provide clarity of the concept and show how BYOD is emerging as a phenomenon.

2.2 Bring Your Own Device (BYOD)

This section will start by providing a definition of bring your own device (BYOD). It will then discuss how this concept has become a norm in organizations and employees' day-to-day work activities. After that, this section will shed light on the expected values and benefits of BYOD for employees and organizations. Finally, it will discuss the risks associated with adopting BYOD.

2.2.1 BYOD Definition

Bring your own device (BYOD) refers to the practice where an organization permits its employees to use their personally-owned devices (e.g., laptops, smartphones, tablets), whether inside or outside of their workplaces, to perform their work tasks. These devices are provided with access to organizations' information systems (e.g., network, applications, and information). This phenomenon is also referred to in the literature as "IT consumerization" (Disterer and Kleiner, 2013; Tokuyoshi, 2013; Crossler et al., 2014; Garba et al., 2015).

2.2.2 BYOD: A New Trend Adopted by Organizations and Employees

Today, BYOD is more of a norm rather than an exception (Crossler et al., 2014; Steelman et al., 2016), possibly due to the growing usage of emerging technologies, and more specifically, mobile technologies. The International Telecommunications Union (ITU) (a United Nations agency) report estimated 3.2 billion internet users around the world and, by the end of 2015, a mobile cellular subscription penetration rate of 97% or more than 7 billion mobile cellular subscriptions (ITU, 2015).

Such personally-owned devices started to be utilized by employees for work-related activities. A 2012 survey of thousands of employees showed that the majority were using their own devices for work (Bradley et al., 2012) due to an increasing belief that it is their right to bring their own devices to work; some even deliberately flouting policies against BYOD (Davis, 2012). Some employees even spend their own money specifically to bring their own devices to

the work environment: “according to Forrester, 33% of us are paying for devices specifically to help us do our jobs better. We purchase these devices for personal use and incorporate them into our work environment – with or without the support of the IT department” (Tokuyoshi, 2013 p.12). A survey in 2018 covering more than 2000 organizations, showed that 45% of employees used personally-owned devices for work (Vaidya, 2018). Therefore, many organizations are expected to move ahead with implementing Bring Your Own Device.

2.2.3 Expected Benefits of BYOD

Many organizations adopt BYOD strategies in the belief that it will provide value to them. Several positive effects of BYOD have been discussed in prior research in terms of improving employees’ satisfaction, providing them with better usability, enabling mobility, increasing efficiency, improving productivity, and lowering operational costs for organizations (e.g., Tokuyoshi, 2013; Crossler et al., 2014; Willis, 2014; Garba et al., 2015; Palanisamy et al., 2020a). Empowering employees to speak for themselves with the freedom to use their own devices is expected to increase job satisfaction; hence, the avoidance of forcing them to use preselected devices that may not satisfy their requirements or taste will result in happier employees (e.g., Thomson, 2012; Disterer and Kleiner, 2013; Moyer, 2013; Willis, 2014; Garba et al., 2015). Some studies have also argued that employees are the ones doing the job and so they will know the most effective tool to do the job; thus, they will bring the devices they believe will have the best usability (e.g., device features, applications) for each of their unique and specific tasks (Tokuyoshi, 2013). Furthermore, with the ever more commonplace expectation that workloads must be completed, even if that means working outside contracted hours and adopting work from home strategies, which leads to the need to always be connected, BYOD allows employees to integrate their devices with organizational information systems and so provides them with the ability to work at any time and from any place (Disterer and Kleiner, 2013). Employees who are satisfied, i.e., using a device of their own choosing with the right usability requirements and able to do their work anywhere and at any time, will be more efficient in their tasks (e.g., Disterer and Kleiner, 2013; Crossler et al., 2014; Garba et al., 2015). Finally, organizations believe that the burden and cost of maintaining devices will be borne by the employees, as they are responsible for maintaining their own devices. This shift of maintenance ownerships is envisaged to reduce the cost of organizational operations (Dang and Pittayachawan, 2015; Garba et al., 2015).

2.2.4 Risks of BYOD

BYOD provides employees with the freedom to use their personally-owned devices at any time and in any place to perform work-related activities (Disterer and Kleiner, 2013). It also allows them to use their devices in their work environments to perform personal activities (e.g., social media, personal email) (Disterer and Kleiner, 2013; Dang and Pittayachawan, 2015). This freedom is accomplished by integrating employees' personally-owed devices with the organizations' information systems (e.g., network, applications, and information) (e.g., Disterer and Kleiner, 2013; Tokuyoshi, 2013; Crossler et al., 2014; Garba et al., 2015).

However, this freedom does not come without a price: BYOD has also introduced several risks related to organizational information security (Disterer and Kleiner, 2013; Palanisamy et al., 2020a) which, if exploited, can cause loss of organizations' data (Garba et al., 2017). Several aspects of BYOD can trigger these risks, including device management, access control, loss of device, hacking, malware, device theft, and apps used by users (Garba et al., 2015; Garba et al., 2017). Although some organizations recognize and understand BYOD-related risks, this does not necessarily mean that their employees do (Doargajudhur and Dell, 2019). The complexity of BYOD and the challenges it poses to organizations have led many to refer to it as "Bring Your Own Danger" (Doargajudhur and Dell, 2019).

Palanisamy et al. (2020b) conducted a systematic review of 17 studies to define BOYD policy compliance risks. The review showed that security risks are continually evolving, putting organizations at risk of information security threats when it comes to adopting BYOD. The review defined 29 BYOD risks that require organizations' attention and grouped them under the people, process, and technology dimensions. Within the people dimension, employee behaviors such as compliance, misuse and carelessness were examples of the risks defined. Within the process dimension, example risks related to lack of policy, employee awareness and training, and in the technology dimension, the examples included device management, malware attacks, and connectivity to risky networks.

Therefore, there is a need to review the extant information security studies to examine how these studies investigated employees' compliance with information security policy in general and how they introduced BYOD in these studies. The next section will aim to perform that review to capture these efforts and illustrate the general direction taken by these studies.

2.3 Information Security Behavioral Studies

This section will discuss the different studies conducted by prior researchers that investigated the behavioral aspects of information security. In this discussion, a detailed review will be conducted of the different theories used to study employees' behaviors when it comes to complying with information security and the outcome of these studies. At the end of this section, the review will focus on those studies that investigated employee compliance with information security behaviors in relation to BYOD.

2.3.1 Previous Employee Information Security Behaviors Studies

Decision-makers need guidance on the best methods to discourage misuse of their information assets and achieve compliance with information security policies within organizations and the appetite for such guidance increases over time as organizations adopt new technologies and strategies in the ICT fields such as BYOD (Bulgurcu et al., 2010a). Several studies aimed to understand employees' behaviors related to compliance with information security policies in order to address the information security needs of these organizations and offer insights and possible solutions (e.g., Siponen et al., 2007; Herath and Rao, 2009a; D'Arcy and Herath, 2011).

A review of previous studies on information security behaviors will be performed to capture their results and conclusions. Further, the review will also focus on how BYOD was introduced in these studies. Other researchers have previously carried out similar reviews to provide an overview of what has been covered in this field. Siponen (2005) reviewed information security literature, focusing on the different approaches used to implement information security and comparing their underlying assumptions; however, in his review, little attention was paid to information security policy compliance behaviors. Siponen and Oinas-Kukkonen (2007) also followed a similar approach in conducting their review of security issues—where they focused on the development of secure information systems, security management, secure communication, and access to information systems—but not on employees' behaviors regarding compliance with information security policies. Padayachee (2012) conducted a systematic review of studies related to compliance with information security policies and produced a taxonomy of factors relevant to employees' behaviors when it comes to adhering to these policies. D'Arcy and Herath (2011) gave a more focused review of employees' behaviors by conducting a systematic review of 17 studies that had applied deterrence theory, and highlighted critical issues with its application; they also put forward recommendations and

guidelines for future research. Sommestad et al. (2014) conducted a systematic review of 29 studies, which: 1) studied variables influencing information security policy compliance; 2) were empirically tested; and, 3) published in a peer-reviewed publication. They identified around 60 variables that influence information security behaviors and concluded that there is no clear 'winner'; each of the variables explains a small amount of the variance in behavior, and each showed variation in different studies. Alaskar et al. (2015) conducted another systematic review in which they identified 36 empirical studies of information security behaviors. They only focused on studies that explicitly mentioned information security policy terms and excluded studies that used different terms which might not be understood as security concerns by the participants—for example, internet policy misuse. Also, they distinguished between studies in which the behaviors in question were positive, such as complying with information security polices, or negative, such as misusing organizations' assets. They also highlighted the theoretical and methodological development related to employees' information security behaviors in addition to showing empirical studies' dissemination in academic journals. Such reviews provide researchers with a starting point to perform their studies in related fields.

Building on the previous reviews, this study aims to expand the coverage to include other studies that may not have previously been covered. Such studies might be more recently published (e.g., Humaidi and Balakrishnan, 2015; Ifinedo, 2016), not covered in these reviews (e.g., D'Arcy et al., 2014), or more specific to the information security of BYOD (e.g., Crossler et al., 2014; Dang and Pittayachawan, 2015). The focus will be on papers that studied the behaviors related to information security.

Based on the review of the literature, this thesis identified 55 studies that have investigated employees' behaviors when it comes to complying with or violating information security policy (see Appendix A) and categorized them accordingly. The first category includes 36 studies that investigated positive employee behaviors related to information security (e.g., compliance). In comparison, the second category consists of 19 studies that investigated negative information security employee behaviors (e.g., abuse and misuse).

The review showed that protection motivation was the theory most used in these studies in order to investigate and explain employees' information security behaviors. Of the 31 studies that used this theory, 28 investigated positive employee behaviors (i.e., Siponen et al., 2006; Pahnila et al., 2007b; Pahnila et al., 2007a; Siponen et al., 2007; Boss et al., 2009; Herath and

Rao, 2009b; Herath and Rao, 2009a; Bulgurcu et al., 2010a; Johnston and Warkentin, 2010; Siponen et al., 2010; Ifinedo, 2012; Vance et al., 2012; Pahnila et al., 2013; Yoon and Kim, 2013; Siponen et al., 2014; Boss et al., 2015; Johnston et al., 2015; Posey et al., 2015; Safa et al., 2015; Sommestad et al., 2015; Hanus and Wu, 2016; Warkentin et al., 2016; Bélanger et al., 2017; Burns et al., 2017; Menard et al., 2017; Torten et al., 2018; Li et al., 2019; Rajab and Eydgahi, 2019), while the remaining three investigated negative employee behaviors (i.e., Workman et al., 2008; Johnston et al., 2016; Moody et al., 2018).

The review showed that deterrence theory was applied in order to investigate and explain employees' information security behaviors in 30 studies. Of these, 15 investigated positive employee behaviors (i.e., Lee et al., 2004; Pahnila et al., 2007b; Pahnila et al., 2007a; Siponen et al., 2007; Herath and Rao, 2009b; Herath and Rao, 2009a; Bulgurcu et al., 2010a; Siponen et al., 2010; Son, 2011; Chen, 2012; Johnston et al., 2015; Ifinedo, 2016; Aurigemma and Mattson, 2017; Chen et al., 2018; Rajab and Eydgahi, 2019), and 15 negative employee behaviors (i.e., Straub Jr, 1990; Harrington, 1996; Skinner and Fream, 1997; Dugo, 2007; D'Arcy and Hovav, 2009; D'Arcy et al., 2009; Siponen and Vance, 2010; Hu et al., 2011; Guo and Yuan, 2012; Barlow et al., 2013; Cheng et al., 2013; Johnston et al., 2016; Alshare et al., 2018; Moody et al., 2018; Merhi and Ahluwalia, 2019). The application of deterrence theory in information security literature showed a balance between applying it to the two types of behaviors. However, this was also the most used theory when studying negative employee behaviors related to information security.

The third most dominant theory, with 28 studies, was the theory of reasoned action. The application of this theory followed the same approach taken by researchers when applying protection motivation theory, where it was mostly used to study employees' positive information security behaviors. A total of 22 studies applied the theory to explore positive employee information security behaviors (i.e., Siponen et al., 2006; Pahnila et al., 2007b; Pahnila et al., 2007a; Siponen et al., 2007; Bulgurcu et al., 2009; Herath and Rao, 2009b; Herath and Rao, 2009a; Zhang et al., 2009a; Bulgurcu et al., 2010a; Siponen et al., 2010; Hu et al., 2012; Ifinedo, 2012; Al-Omari et al., 2013; Yoon and Kim, 2013; Ifinedo, 2014; Siponen et al., 2014; Safa et al., 2015; Sommestad et al., 2015; Rocha Flores and Ekstedt, 2016; Aurigemma and Mattson, 2017; Bélanger et al., 2017; Rajab and Eydgahi, 2019), while six studies applied the theory when examining negative employee information security behaviors

(i.e., Dugo, 2007; Workman and Gathegi, 2007; Cox, 2012; Cheng et al., 2013; Moody et al., 2018; Merhi and Ahluwalia, 2019).

In addition to the above three theories, others have been applied by more than one study to examine employees' information security behaviors. For example, rational choice theory was used three times for both positive (i.e., Bulgurcu et al., 2010a; Ifinedo, 2016; Han et al., 2017) and negative (i.e., Hu et al., 2011; Vance and Siponen, 2012; Kajtazi et al., 2018) behaviors. The health belief model was used in five studies, four of them examining positive behavior (i.e., Ng et al., 2009; Humaidi and Balakrishnan, 2015; Dodel and Mesch, 2019; Li et al., 2019) and one negative (Moody et al., 2018). Four studies investigating positive information security behaviors applied social cognitive theory (i.e., Ng et al., 2009; Rhee et al., 2009; Ifinedo, 2014; Ahmad et al., 2019) and three studies investigating negative information security behaviors applied neutralization theory (i.e., Siponen and Vance, 2010; Barlow et al., 2013; Moody et al., 2018). Social bond theory was used to study both positive (Ifinedo, 2014; Sohrabi Safa et al., 2016) and negative (Cheng et al., 2013) behaviors. Both involvement theory (Sohrabi Safa et al., 2016; Amankwa et al., 2018) and innovation diffusion theory (Pahnila et al., 2007b; Siponen et al., 2010) were each used in two studies that focused on positive information security behaviors while the theory of interpersonal behavior was used once in a study on positive information security behaviors (Pahnila et al., 2007a) and once on negative information security behaviors (Moody et al., 2018).

In addition, other theories were only used once. For positive employee information security behaviors studies, researchers applied several theories—or variables adopted from these theories—such as cognitive moral development theory (Myyry et al., 2009), five-factor model of personality (Shropshire et al., 2015), DeLone and MacLean theory (Pahnila et al., 2007a), deontological theory (Al-Omari et al., 2013), leadership style theory (Humaidi and Balakrishnan, 2015), motivational types of values theory (Myyry et al., 2009), organization climate theory (Ifinedo, 2016), safety climate theory (Chan et al., 2005), social identity theory (Bulgurcu et al., 2009), technology acceptance theory (Shropshire et al., 2015), Psychological ownership theory (Yoo et al., 2018), self-determination theory (Menard et al., 2017), flow theory (Yoo et al., 2018), and teleological theory (Al-Omari et al., 2013). Theories applied by researchers to investigate negative behaviors included the causal reasoning theory (Posey et al., 2011), composite behavior model (Guo et al., 2011), moral disengagement theory (D'Arcy et al., 2014), social learning theory (Skinner and Fream, 1997), theory of self-regulation

(Moody et al., 2018), extended parallel processing model (Moody et al., 2018), and technostress theory (D'Arcy et al., 2014).

Table 1 provides a summary of key theories used in information security behaviors. It also shows the usage of these theories based on whether it is positive or negative information security behavior.

TABLE 1: KEY THEORIES USED IN PREVIOUS STUDIES ON EMPLOYEES INFORMATION SECURITY BEHAVIOR

Theory Name	Total	Positive Behavior Studies	Positive Behavior Studies	Negative Behavior Studies	Negative Behavior Studies
Protection Motivation Theory	31	Siponen et al. (2006); Pahnila et al. (2007b); Pahnila et al. (2007a); Siponen et al. (2007); Boss et al. (2009); Herath and Rao (2009b); Herath and Rao (2009a); Bulgurcu et al. (2010a); Johnston and Warkentin (2010); Siponen et al. (2010); Ifinedo (2012); Vance et al. (2012); Pahnila et al. (2013); Yoon and Kim (2013); Siponen et al. (2014); Boss et al. (2015); Johnston et al. (2015); Posey et al. (2015); Safa et al. (2015); Sommestad et al. (2015); Hanus and Wu (2016); Warkentin et al. (2016); Bélanger et al. (2017); Burns et al. (2017); Menard et al. (2017); Torten et al. (2018); Li et al. (2019); Rajab and Eydgahi (2019)	28	Workman et al. (2008); Johnston et al. (2016); Moody et al. (2018)	3
Deterrence Theory	30	Lee et al. (2004); Pahnila et al. (2007b); Pahnila et al. (2007a); Siponen et al. (2007); Herath and Rao (2009b); Herath and Rao (2009a); Bulgurcu et al. (2010a); Siponen et al. (2010); Son (2011); Chen (2012); Johnston et al. (2015); Ifinedo (2016); Aurigemma and Mattson (2017); Chen et al. (2018); Rajab and Eydgahi (2019)	15	Straub Jr (1990); Harrington (1996); Skinner and Fream (1997); Dugo (2007); D'Arcy and Hovav (2009); D'Arcy et al. (2009); Siponen and Vance (2010); Hu et al. (2011); Guo and Yuan (2012); Barlow et al. (2013); Cheng et al. (2013); Johnston et al. (2016); Alshare et al. (2018); Moody et al. (2018); Merhi and Ahluwalia (2019)	15

TABLE 1: KEY THEORIES USED IN PREVIOUS STUDIES ON EMPLOYEES INFORMATION SECURITY BEHAVIOR CONT'D

Theory Name	Total	Positive Behavior Studies	Positive Behavior Studies	Negative Behavior Studies	Negative Behavior Studies
Theory of Reasoned Action/Theory of Planned Behavior	29	Siponen et al. (2006); Pahnila et al. (2007b); Pahnila et al. (2007a); Siponen et al. (2007); Bulgurcu et al. (2009); Herath and Rao (2009b); Herath and Rao (2009a); Zhang et al. (2009a); Bulgurcu et al. (2010a); Siponen et al. (2010); Hu et al. (2012); Ifinedo (2012); Al-Omari et al. (2013); Yoon and Kim (2013); Ifinedo (2014); Siponen et al. (2014); Safa et al. (2015); Sommestad et al. (2015); Rocha Flores and Ekstedt (2016); Aurigemma and Mattson (2017); Bélanger et al. (2017); Rajab and Eydgahi (2019)	22	Dugo (2007); Workman and Gathegi (2007); Cox (2012); Cheng et al. (2013); Moody et al. (2018); Merhi and Ahluwalia (2019)	6
Rational Choice Theory	6	Bulgurcu et al. (2010a); Ifinedo (2016); Han et al. (2017)	3	Hu et al. (2011); Vance and Siponen (2012); Kajtazi et al. (2018)	3
Health Belief Model	5	Ng et al. (2009); Humaidi and Balakrishnan (2015); Dodel and Mesch (2019); Li et al. (2019)	4	Moody et al. (2018)	1
Social Bond Theory	3	Ifinedo (2014); Sohrabi Safa et al. (2016)	2	Cheng et al. (2013)	1

TABLE 1: KEY THEORIES USED IN PREVIOUS STUDIES ON EMPLOYEES INFORMATION SECURITY BEHAVIOR CONT'D

Theory Name	Total	Positive Behavior Studies	Positive Behavior Studies	Negative Behavior Studies	Negative Behavior Studies
Innovation Diffusion Theory	2	Pahnila et al. (2007b); Siponen et al. (2010)	2	-	-
Involvement Theory	2	Sohrabi Safa et al. (2016); Amankwa et al. (2018)	2	-	-
Theory of Interpersonal Behavior	2	Pahnila et al. (2007a)	1	Moody et al. (2018)	1
Big Five Personality Traits	1	-	-	Johnston et al. (2016)	1
Causal Reasoning Theory	1	-	-	Posey et al. (2011)	1
Social Learning Theory	1	-	-	Skinner and Fream (1997)	1
Technology Acceptance Theory	1	Shropshire et al. (2015)	1	-	-

These reviews also show that most of the studies did not apply one theory in Isolation but used variables from several theories to address their research question(s). For example, Bulgurcu et al. (2010a) applied deterrence theory, protection motivation theory, theory of reasoned action, and rational choice theory to define employees' beliefs about thier assessment of the outcome of compliance or noncompliance with the information security policy, which affects their attitude towards compliant behavior and, thus, intention to comply. They also aimed to explain the effect of information security awareness on the beliefs employees have about compliance or noncompliance outcomes. Such an application was followed by most of the identified studies.

During the search for behavioral information security studies, other studies were identified, some of which had been included in previous reviews by other authors. These studies were not included in Table 1 since they were not explicitly information security behavioral studies. Some are arguably related to information security since some information security policy is covered in them. However, to illustrate the reason for excluding articles, asking respondents to respond to the question ("Are you intending to comply with the internet policy in your organization?") will be perceived differently from the question ("Are you intending to comply with the information security policy?"). Therefore, in Table 1, the review only included studies that were explicitly about information security. Some of these related to privacy policy (Johnston and Warkentin, 2008; Warkentin et al., 2011), access policy (Vance et al., 2013), internet policy (Liao et al., 2009; Li et al., 2010), adopting security technology (Lee and Larsen, 2009; Cheng and Shi-bo, 2014) and piracy (Gopal and Sanders, 1997; Lin et al., 1999; Peace et al., 2003; Higgins et al., 2005; Zhang et al., 2009b; Siponen et al., 2012).

Table 2 describes all of the main theories identified in this literature review. The review of the main theories adopted in the information security literature provides the foundation to understand the underlying assumptions of these theories better, how they were adopted and their contribution to the body of knowledge when it comes to explaining individuals' behaviors.

TABLE 2: DESCRIPTIONS OF THEORIES IN EMPLOYEE INFORMATION SECURITY BEHAVIORAL STUDIES

Theory Name	References	Description	Field	Main Constructs
Protection Motivation Theory	Rogers (1975); Rogers (1983); Rogers and Prentice-Dunn (1997); Floyd et al. (2000)	Protection motivation theory posits that individuals will perform a protection-related behavior based on their threat appraisal (consisting of Perceived Threat Vulnerability, Perceived Threat Severity, and Rewards) and coping appraisal (consisting of Response Efficacy, Self-Efficacy, and Response Cost).	Health Communication	Perceived Threat Vulnerability, Perceived Threat Severity, Rewards, Response Efficacy, Self-Efficacy, Response Cost
Deterrence Theory	Gibbs (1975); Gibbs (1979)	The Deterrence theory posits that individuals will avoid performing a criminal activity based on their perception of punishment. This perception includes the certainty of sanctions, the severity of sanctions, and the celerity of sanctions.	Criminology	Perceived Certainty of Sanctions, Perceived Severity of Sanctions, Perceived Celerity of Sanctions
Theory of Reasoned Action/ Theory of Planned Behavior	Fishbein and Ajzen (1975); Ajzen (1991); Fishbein (2000); Fishbein and Ajzen (2010)	The theory of reasoned action posits that individuals perform behaviors based on their intention to perform this behavior and their actual ability to perform this behavior. The intention is formulated based on individuals' attitudes toward this behavior, the social norm perceived by the individual, and the individual's perception of the extent of their control over the behavior.	Health Communication and Psychology	Attitude, Social Norms, Perceived Behavioral Controls
Rational Choice Theory	Becker (1968); McCarthy (2002)	Rational choice theory posits that individuals perform a rational calculation in their decision making. In this calculation, they weigh benefits against the cost to achieve their objectives, calculating the highest benefits and the lowest costs. Accordingly, they may perform a certain behavior or not.	Economy and Criminology	Benefits, Cost

TABLE 2: DESCRIPTIONS OF MAIN USED THEORIES IN EMPLOYEES INFORMATION SECURITY BEHAVIORAL STUDIES CONT'D

Theory Name	References	Description	Field	Main Constructs
Health Belief Model	Becker (1974); Rosenstock (1974)	The health belief model posits that for individuals to perform a health-related behavior, they will evaluate the threat of the disease and the expected benefits from the behavior and the barriers to performing the behavior when triggered by some cues to action.	Health Communication	Perceived Threat (consists of Perceived Susceptibility and Perceived Severity), Perceived Benefits, Perceived Barriers, Cues to Action
Social Cognitive Theory	Bandura (1986)	The social cognitive theory posits that for individuals to perform a behavior, they undertake a cognitive process based on the interaction of the behavior, the personal factors, and the environmental factors.	Psychology	Behavior, Environmental Factors, Personal Factors
Neutralization Theory	Sykes and Matza (1957)	Neutralization theory posits that individuals use different techniques to justify rule-breaking behaviors to themselves, whether these rules are laws, social norms, or personal beliefs. Individuals may use one or a combination of these techniques.	Criminology	Denial of Responsibility, Denial of Injury, Denial of Victim, Condemn the Condemners, Appeal to Higher Loyalties, Metaphor of the Ledger, and Defense of Necessity
Social Bond Theory	Hirschi (1969)	Social bond theory posits that individuals depend on their ties with their social surroundings when deciding whether or not to perform deviant activities. The theory defined the social bond as having four factors: attachment, commitment, involvement, and personal norms.	Criminology	Attachment, Commitment, Involvement, and Personal Norms

2.3.2 Review of Theoretical Application in Information Security Studies

2.3.2.1 Protection Motivation Theory (PMT) in Information Security Studies

In 1975, Ronald W. Rogers proposed the protection motivation theory (Rogers, 1975). Rogers aimed to provide a better understanding of fear appeal and its role in changing people's attitudes to cope with their fear appeals. The fear appeal in protection motivation theory is composed of the magnitude of noxiousness of the event, the occurrence probability of the event, and the efficacy of the recommended response, which will either eliminate or reduce the noxiousness of the event. Protection motivation theory argues that a cognitive process mediates the effect of fear appeal on people's attitudes: people go through this process to evaluate the exposure due to the event, the severity of exposure due to the event, and the efficacy of the recommended coping response, which arouses a protection motivation that will influence any change in attitude. Protection motivation is defined as "an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity" (Rogers, 1975, p.98).

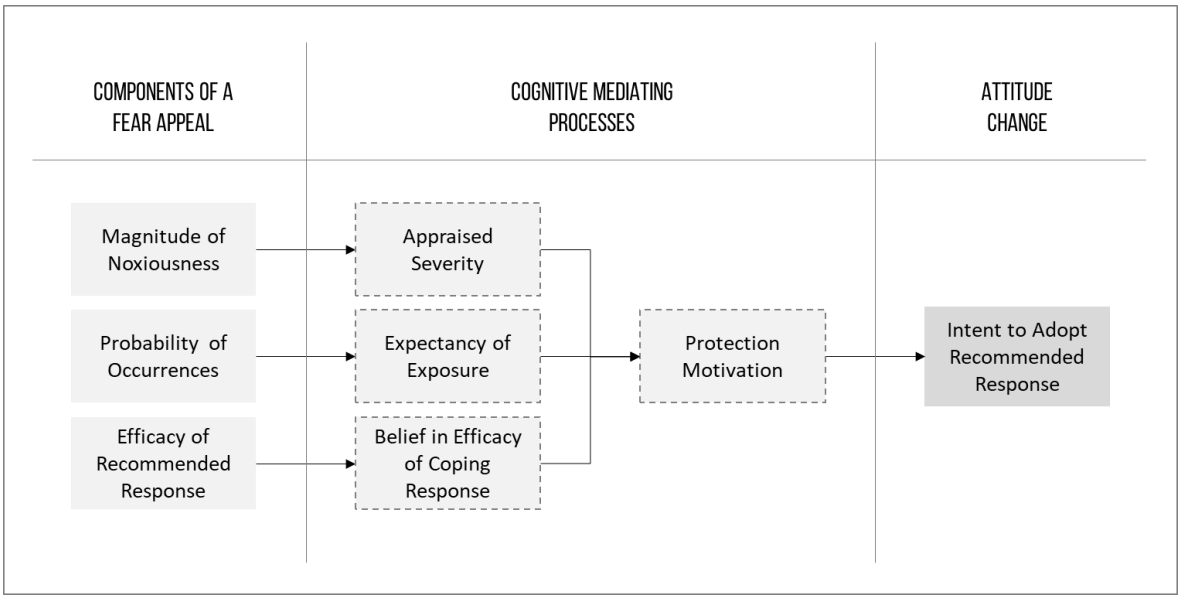


FIGURE 2: SCHEMA OF THE PROTECTION MOTIVATION THEORY

(ROGERS, 1975, P.99, FIG. 1)

In 1983, Rogers revised the protection motivation theory by extending it into a theory of persuasive communication. The revised model focused on the cognitive mediating process and argues that different types of information sources may initiate the cognitive process. The sources of information can be either environmental (e.g., verbal persuasion or observational learning) or interpersonal (e.g., personality variables or prior experience) (Rogers, 1983).

Further, the revised model argues that the cognitive process mediates the effect of these information sources on different coping modes (Rogers, 1983). This cognitive mediating process is composed of two appraisals, threat and coping, resulting in the formation of protection motivation. Each appraisal evaluates the factors involved: threat appraisal is concerned with evaluating intrinsic and extrinsic rewards (i.e., factors increasing the response probability) against the threat of severity and vulnerability of the threat (i.e., factors decreasing the response probability) while coping appraisal is concerned with evaluating response efficacy and self-efficacy (i.e., factors increasing the response probability) against response cost (i.e., factors decreasing the response probability). The resulting protection motivation variable affects people's coping modes, which lead either to performing the action or not performing the action.

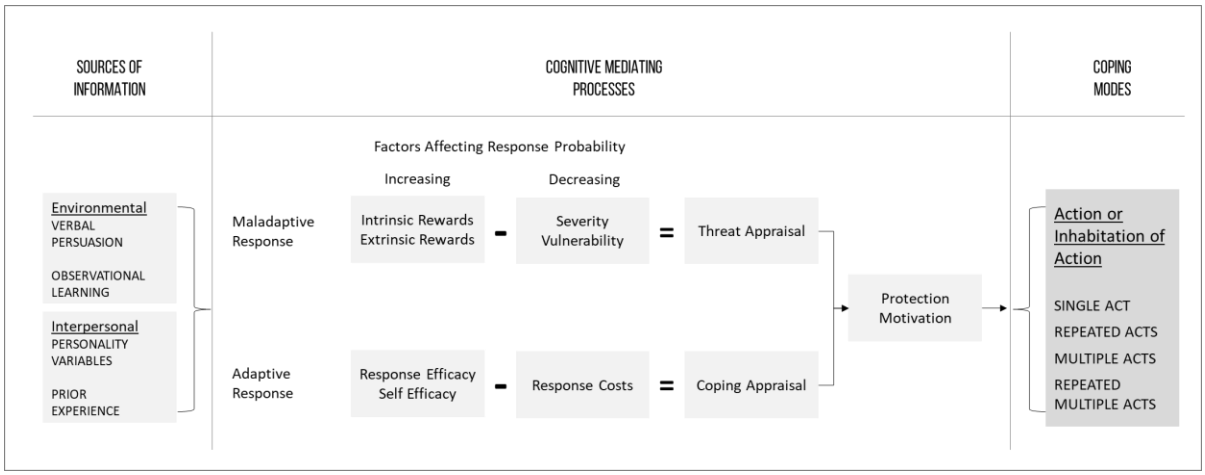


FIGURE 3: SCHEMA OF THE REVISED PROTECTION MOTIVATION THEORY

(Rogers, 1983, p.168, Fig. 6-2)

In a study by Workman et al. (2008), the omission of security behavior was tested both subjectively (i.e., self-reporting intention) and objectively (i.e., actual behavior by examining the computer logs). The results from 588 employees presented a significant negative impact of perceived threat vulnerability, perceived threat severity, response efficacy, response cost, and self-efficacy variables on both subjective and objective omissions of security.

Another study hypothesized that both threat appraisal (i.e., perceived threat vulnerability and perceived threat severity) and coping appraisal (i.e., self-efficacy and response efficacy) have a positive impact on employees' intention to comply with the information security policy: its analysis of 919 employees' responses from five Finnish companies provided support for these hypotheses (Siponen et al., 2006). Additionally, Siponen et al. (2007) found that threat

appraisal (including both perceived threat severity and perceived threat vulnerability), self-efficacy, and response efficacy are significant. These three studies showed significant results for all of the protection motivation theory variables tested.

The remaining studies that have investigated employees' compliance behaviors using protection motivation theory have provided support to some of the variables but not to all. Johnston and Warkentin (2010), with a sample size of 275, included four variables from protection motivation theory (perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy). Their results showed that only perceived threat vulnerability was insignificant, whereas the other variables were significant. Vance et al. (2012) examined the effect of the perceived threat vulnerability, perceived threat severity, response efficacy, response cost, and self-efficacy variables on employees' intention to comply with the information security policy in their organizations. The study covered 111 information security experts and managers and came to similar conclusions to those of Johnston and Warkentin (2010) in that all of the variables from protection motivation theory were significant, except for perceived threat vulnerability.

In contrast, other studies have shown the significance of perceived threat vulnerability but failed to show the significance of one or more other variables. Ifinedo (2012) tested the effect of the perceived threat vulnerability, perceived threat severity, response efficacy, response cost, and self-efficacy variables on employees' intention to comply with the information security policy. The study covered 124 business managers and information systems professionals, and showed that all of the protection motivation theory factors, including perceived threat severity are significant, except for response cost, which was not; however, perceived threat severity had a significant negative effect on employees' intention, which did not support the hypothesis.

Moreover, Siponen et al. (2010) showed that both self-efficacy and threat appraisal (combining both perceived threat vulnerability and perceived threat severity) had a significant effect on employees' intention to comply with the information security policy, whereas response efficacy was insignificant. Pahnila et al. (2007a) found similar results, while Siponen et al. (2007) found almost similar results with exception of response efficacy which was significant.

Additionally, in a study covering 312 employees from 78 organizations, variables from protection motivation theory (i.e., perceived threat vulnerability, perceived threat severity, response efficacy, response cost, and self-efficacy) were tested for their impacts on employees'

compliance with information security policy behavior (Herath and Rao, 2009b). With the exception of self-efficacy, significance was identified for the effect of the protection motivation theory variables on the employees' intention.

Further, Lee and Larsen (2009) investigated the impact of protection motivation theory on executives' intention to adopt anti-malware software. A multi-group analysis on a sample size of 239 was conducted with four groups: 1) information security experts, 2) non-information security experts, 3) IT-intensive industry, and 4) non-IT intensive industry. Perceived threat severity and response cost were significant in all of the groups. Perceived threat vulnerability was significant only in the information security expert group and the IT-intensive industry groups. Response efficacy and self-efficacy were only significant in the non-information security expert group and the non-IT-intensive industry groups. Although, with one exception, the studies in the review showed perceived threat vulnerability to be significant, the remaining PMT variables (i.e., perceived threat severity, rewards, response efficacy, self-efficacy, and response cost) were found to have a significant influence on the intention to comply with the information security policy (Vance et al., 2012).

Other studies used the main variables from protection motivation theory to study their impacts on employees' intention to comply with the information security policy through their attitudes toward compliance behaviors. In Yoon and Kim's (2013) study, perceived threat severity, response efficacy, and self-efficacy significantly affected employees' attitudes, whereas perceived vulnerability was insignificant. Pahnila et al. (2007a) showed threat appraisal (i.e., perceived threat vulnerability and perceived threat severity) to be significant, whereas coping appraisal (i.e., self-efficacy and response efficacy) was found to be insignificant.

2.3.2.2 Deterrence Theory (DT) in Information Security Studies

The origin of deterrence theory can be traced back to Cesare Beccaria, referred to by many as the father of classical criminology. His work *On Crimes and Punishments* (1764) is considered to be the root from which deterrence theory has grown (Onwudiwe et al., 2005). According to Beccaria (2013), humans have free will to make their own decisions which are made based on a rational calculus. Beccaria argued that people go through this rational calculus when deciding whether to conduct a crime, to weigh up the advantages expected from committing the crime and the disadvantage of punishment. He argued that milder punishments are required, rather than cruel ones, and that the punishment should not exceed what makes people lean toward not

committing the crime when they go through this rational calculus, arguing that "the certainty of small punishment will make a stronger impression, than the fear of one more severe" (2013, p.63).

Drawing from Beccaria's work, deterrence theory posits that if the punishment outweighs the anticipated benefits of committing the crime, then the crime will not be committed (Akers, 1990; D'Arcy and Herath, 2011). As people go through the rational calculus of whether to commit or not commit the crime, three main components are taken into consideration: 1) the severity of the punishment, 2) the certainty of the punishment, and 3) the celerity of the punishment (Gibbs, 1975; Gibbs, 1979). The severity of the punishment is referred to as "the perceived degree of punishment for the intended act" (Hu et al., 2011, p.57). The theory of deterrence hypothesizes that the more severe the punishment, the better the deterrence effect (Siponen et al., 2012). The second component, the certainty of the punishment, refers to "the perceived probability of being punished for the intended act" (Hu et al., 2011, p.57), where the higher the risk of being caught, the higher the deterrence effect (Siponen and Vance, 2010). The third component is concerned with "the perceived swiftness of being punished for the intended act" (Hu et al., 2011, p.57), where the higher the celerity of punishment, the greater the deterrence effect (D'Arcy and Herath, 2011). Thus, the higher the impact of the severity, certainty, and celerity of the punishment for committing a crime is, the higher the chances that the individual will not commit the crime (Williams and Hawkins, 1986).

The applications of deterrence theory in information security studies consist of investigating both positive and negative behaviors as presented in Table 1. Positive behaviors are those concerned with doing the right thing (e.g., compliance with a policy or appropriate usage of information systems (i.e., Lee et al., 2004; Pahnila et al., 2007b; Pahnila et al., 2007a; Siponen et al., 2007; Herath and Rao, 2009b; Herath and Rao, 2009a; Bulgurcu et al., 2010a; Siponen et al., 2010; Son, 2011; Chen, 2012; Johnston et al., 2015; Ifinedo, 2016; Aurigemma and Mattson, 2017; Chen et al., 2018; Rajab and Eydgahi, 2019). In contrast, negative behaviors are those concerned with doing the 'wrong' thing (e.g., misusing the information system or not complying with the information security policy (i.e., Straub Jr, 1990; Harrington, 1996; Skinner and Fream, 1997; Dugo, 2007; D'Arcy and Hovav, 2009; D'Arcy et al., 2009; Siponen and Vance, 2010; Hu et al., 2011; Guo and Yuan, 2012; Barlow et al., 2013; Cheng et al., 2013; Johnston et al., 2016; Alshare et al., 2018; Moody et al., 2018; Merhi and Ahluwalia, 2019).

These studies covered both behaviors related to complying with information security policy and other behaviors that fall under information security in general.

Many studies provided support to deterrence theory with regard to compliance with information security policy. Siponen et al. (2010) deployed a single variable named deterrence, which is a combination of the three variables of severity, certainty, and celerity of punishment. A test of 917 employees' responses showed that deterrence has a significant effect on employees' actual compliance with the information security policy. The same variable had also previously been used by the same authors in prior research, with a different research model, and the same results regarding deterrence were found (Pahnila et al., 2007b; Siponen et al., 2007).

Bulgurcu et al. (2010a) investigated the impact of both formal and informal sanctions (composed of both formal and informal sanctions, i.e., intrinsic cost) on employees' perception of the cost of noncompliance, and showed that this relationship is significant. The study also showed that the cost of non-compliance has a significant effect on employees' attitudes toward complying. Further, the employees' attitude had a significant impact on employees' intention to comply with the information security policy in their organizations.

Other studies regarding employees' compliance with the information security policy did not provide support to some or all of the deterrence constructs that were tested. Herath and Rao (2009b) studied the effect of both punishment severity and punishment certainty on employees' intention to comply with information security policy. Their findings show that only punishment certainty is significant; punishment severity is insignificant. An earlier paper of theirs showed the same results concerning punishment certainty; however, in this paper, punishment severity was significant, but it had a negative relationship with intention to comply (Herath and Rao, 2009a). This result implies that the lower the severity of punishment is, the higher the employees' intent to comply with the information security policy will be. Therefore, this result did not support the authors' hypothesis, nor does it align with deterrence theory logic.

Li et al. (2010) conducted a study to examine the reasons behind employees' intent to comply with internet usage policy. Severity and certainty of punishment from deterrence theory were hypothesized to be positively affecting employees' intent to comply with internet usage policy. The results supported the effect of the certainty of punishment, but the severity was found to be insignificant. Kankanhalli et al. (2003) studied the deterrent severity and deterrent effort

(i.e., reflecting deterrence certainty) on information systems security effectiveness. In this study, 63 responses were collected from information systems managers responsible for information security in their organizations. The results of the study showed that only deterrent effort was significant. However, Pahnila et al. (2007a) found sanctions (the combination of severity and certainty) to be of insignificant influence on employees' intentions to comply with the information security policy.

When it comes to violation behaviors, Straub (1990) showed that computer abuse behavior is impacted negatively by both certainty and severity of punishment. Similarly, Gopal and Sanders (1997) showed that deterrence information (representing both severity and certainty of punishment) has a significant impact on intent to perform software piracy.

Similar to the information security policy compliance studies, the literature from the violation behaviors stream also did not provide support to some deterrence constructs that were tested. D'Arcy et al. (2009) studied the impact of the certainty and severity of punishment on information security misuse: their analysis of 269 responses showed that only the severity of punishment had a significant negative effect on employees' intentions to misuse information systems.

Higgins et al. (2005) tested the effect of certainty and severity of punishment on software piracy intention, collecting data from 382 students. The results showed that the severity of punishment was insignificant, whereas the certainty of punishment had a significant negative impact on software piracy intention. Similarly, Zhang et al. (2009b) showed that punishment certainty had a significant impact on digital piracy behavior, whereas punishment severity was found to be insignificant. Skinner and Fream (1997) conducted a study on five illegal computing activities: software piracy, password guessing to gain unauthorized access, unauthorized access (i.e., illegal access), unauthorized alteration of content, and creating and using malware software. The study collected data from 581 students for the past month, past year, and lifetime. Two factors from deterrence theory, certainty of punishment, and severity of punishment were tested against these five illegal activities. The results of the data analysis showed that both factors were insignificant, apart from severity which was significant with unauthorized access.

Other literature on violation behaviors does not show much support for deterrence theory. Siponen and Vance (2010) investigated the impacts of both formal (e.g., salary deduction) and informal punishments (e.g., guilt) on employees' intent to violate information security policy.

The informal punishment consisted of two variables: the informal punishment variable as normally used in other studies (e.g., disapproval of peers), and shame. Each of these three variables has been operationalized to include both the certainty and severity aspects of deterrence. After analyzing the data collected from 395 employees, the results showed that only informal punishment was significant; the two remaining variables were insignificant. Another study on employees' intentions to commit information security policy violations was conducted in five companies in China (Hu et al., 2011) where a total of 207 responses were collected and tested. The results showed that certainty, severity, and celerity of punishment were all insignificant. Similarly, another paper by Siponen et al. (2012) showed that formal punishment composed of certainty and severity had insignificant effects on people's intentions to commit software piracy.

Although the deterrence theory has been widely used in the information security literature, the literature review did not identify any BYOD-focused study that used deterrence theory.

2.3.2.3 Theory of Reasoned Action (TRA) in Information Security Studies

The theory of reasoned action argues that an individual's performance of certain behaviors is derived from his/her intention regarding that behavior (Fishbein and Ajzen, 1975; Fishbein and Ajzen, 2010). It also states that actual behavioral control affects the actual performance of the behavior. Such controls, whether in the form of requisite resources (e.g., skills, abilities, strength, and funds) or of opportunities (e.g., the occurrence of events or external barriers), will either prevent the individual from performing the behavior or allow him/her to perform the behavior. However, since it is difficult to measure actual behavioral control, the theory substitutes perceived behavioral control for it (Ajzen, 1991).

TRA posits that the individual's attitude toward the behavior, the perceived norms relating to the behavior, and the perceived behavioral control are the factors that affect the individual's intention. Attitude is defined as the "person's favorable or unfavorable evaluation of the object" (Fishbein and Ajzen, 1975, p.12), where the object refers to the individual's behavior. Descriptive norms ("the observed or inferred actions of those important social referents" (Ajzen, 2012, p.17)) and subjective norms ("individual's perception of what people important to them think about a given behavior" (Ifinedo, 2012, p.85)) are referred to as perceived norms (Fishbein and Ajzen, 2010; Ajzen, 2012). Perceived behavioral control is defined as "people's

perception of the ease or difficulty of performing the behavior of interest" (Ajzen, 1991, p.183), and it is similar to Bandura's (1977) self-efficacy construct.

Further, TRA argues that attitudes, perceived norms, and perceived behavioral control are determined by the beliefs that an individual has about the behavior. Attitude is determined by behavioral beliefs, which is the individual's belief regarding the consequence of the behavior (Fishbein and Ajzen, 1975). Perceived norms are determined by the normative beliefs the individual has about the behavior, and those beliefs manifest as result of the information available about the social pressure for conducting or not conducting the behavior (Fishbein and Ajzen, 1975). Perceived behavioral control is derived from an individual's control belief about the "presence or absence of requisite resources and opportunities" (Ajzen, 1991, p.186).

Within the information security literature, many researchers have deployed TRA to investigate individuals' behaviors related to compliance with the information security policy as shown in Table 1 (i.e., Siponen et al., 2006; Dugo, 2007; Pahnila et al., 2007b; Pahnila et al., 2007a; Siponen et al., 2007; Workman and Gathegi, 2007; Bulgurcu et al., 2009; Herath and Rao, 2009b; Herath and Rao, 2009a; Zhang et al., 2009a; Bulgurcu et al., 2010a; Siponen et al., 2010; Cox, 2012; Hu et al., 2012; Ifinedo, 2012; Al-Omari et al., 2013; Cheng et al., 2013; Yoon and Kim, 2013; Ifinedo, 2014; Siponen et al., 2014; Safa et al., 2015; Sommestad et al., 2015; Rocha Flores and Ekstedt, 2016; Aurigemma and Mattson, 2017; Bélanger et al., 2017; Moody et al., 2018; Merhi and Ahluwalia, 2019; Rajab and Eydgahi, 2019). In Bulgurcu et al.'s (2010a) study, an analysis of 464 employees' responses showed that attitude, normative beliefs, and self-efficacy positively affected employees' intention to comply with the information security policy. Similarly, another study with responses from 124 business managers and information systems professionals supported the same results (Ifinedo, 2012). Likewise, Al-Omari et al. (2013) conducted a study on a sample size of 445, consisting of employees working at seven banks in Jordan; the results were also consistent with the previous studies, where attitude, subjective norms, and self-efficacy were found to positively affect employees' intentions to comply. Another two studies included only two variables from the reasoned action theory (i.e., self-efficacy and normative beliefs); 917 responses from four companies in different businesses showed that both normative beliefs and self-efficacy have a positive impact on employees' intentions to comply with information security policy (Pahnila et al., 2007b; Siponen et al., 2010). Sommestad et al. (2015) also deployed the theory of reasoned action showing attitude, perceived norms, and perceived behavioral control

significantly affecting employees' compliance based on analyzing the results of data collected from 306 employees in Sweden.

Some other studies did not support some of the variables in the theory of reasoned action. Herath and Rao (2009b), in a study covering 312 employees from 78 organizations, showed that subjective norms, descriptive norms, and self-efficacy were significant, whereas attitude was found to be insignificant. In contrast, Zhang et al. (2009a) found attitude and perceived behavioral controls to be significant; however, subjective norms were not significant.

In general, existing empirical evidence demonstrates strong support for the explanation power of this theory. However, some studies have inconsistent findings, suggesting that the relative importance of key factors in explaining behavioral intention might vary in different behavioral contexts. Further, no study has been identified in information security behavior studies related to BYOD in the context of information security.

2.3.2.4 Rational Choice Theory (RCT) in Information Security Studies

Rational choice theory was developed and brought into the criminology literature with an economist perspective (Becker, 1968). Its underlying assumption is that individuals make their decisions based on a rational calculation to achieve their objectives with the highest utility and the lowest cost. This occurs by weighing benefits against the cost. Both benefits and costs can be materialistic, such as money, or non-materialistic, such as psychological. This rational process also affects whether a specific individual performs a particular behavior or not (McCarthy, 2002).

In information security policy compliance studies, several studies applied rational choice theory (e.g., Hu et al., 2011; Ifinedo, 2016; Kajtazi et al., 2018). Bulgurcu et al. (2010a) used the theory to explain how employees form their intention to comply with information security policy, examining what effect the benefits of compliance, cost of compliance, and cost of non-compliance had on their attitude. The three variables significantly affect employees' attitude, which in turn significantly affects their intention. Another study found a significant effect of perceived benefits on employees' intention to comply with the information security policy whereas the perceived cost did not have any significant effect on employees' intentions (Han et al., 2017). Vance and Siponen (2012) utilized the theory to examine employees' intent to violate information security policy and found that both informal sanctions and perceived benefits affect employees' intentions to violate while formal sanctions did not have any effect.

The few examples covered here show that the results of the variables adopted from rational choice theory vary in information security behavioral studies.

2.3.2.5 Health Belief Model (HBM) in Information Security Studies

The health belief model was developed in the health domain to explain and predict individuals' health-related behaviors (Becker, 1974; Rosenstock, 1974). The model states that an individual will undertake health-related behaviors if the individual believes that a negative health condition will be avoided if s/he can undertake the behavior in question successfully. In this process, the individual will evaluate the perceived threat of the disease (which consists of perceived susceptibility and perceived severity), perceived benefits of the behaviors, perceived barriers to performing the behaviors, and the cues to action (e.g., media, advice, etc.).

In the information security behavioral studies reviewed, several studies applied this model, or variables from it, with the assumption that the behavior in question is related to avoiding information security breaches instead of preventing diseases (Ng et al., 2009; Humaidi and Balakrishnan, 2015; Moody et al., 2018; Dodel and Mesch, 2019; Li et al., 2019). In one study, perceived susceptibility and perceived benefits were found to impact employees' computer security behavior, and perceived severity to have a moderating effect on the relationship between perceived benefits and cues to action. In contrast, perceived barriers and cues to action did not have any effect (Ng et al., 2009). In another study, perceived susceptibility and perceived benefits were found to affect employees' intention to perform non-compliant behavior regarding the information security policy while perceived severity was not (Moody et al., 2018). Examples of inclusion of health belief model variables exist in several information security behavior studies with different results for the effect of these variables.

2.3.2.6 Social Cognitive Theory (SCT) in Information Security Studies

Social cognitive theory is one of the key theories that aim to predict and change human behavior. It was originally developed in the 1980s as an extension of social learning theory, but, as reflected in its name, with a substantial emphasis on the cognitive process (Bandura, 1986). The theory aims to understand human behavior, predict these behaviors and define methods to change them. According to the theory, the interaction between behavior, personal factors, and environmental factors formulate individual behavior. Environmental factors are those external to individuals, such as social (e.g. family, friends, etc.) and physical (e.g., location, temperature, etc.). Personal factors include aspects such as beliefs, expectations, and

goals. The behavior in social cognitive theory is assumed to occur and be learned by the individual vicariously which allows the individual to predict the outcome of the behavior. These three factors (behavior, personal and environmental) are assumed to interact with and affect each other and as a result, the behavior might be actioned. The theory has been used to predict many behaviors and intentions related to health (Armitage and Conner, 2000).

Several information security behavioral studies have deployed social cognitive theory (Ng et al., 2009; Rhee et al., 2009; Ifinedo, 2014; Ahmad et al., 2019). Ahmad et al. (2019), found inconvenience, information security monitoring, outcome expectation, self-efficacy, and subjective norms to affect employees' behaviors. Similarly, Rhee (2009) found self-efficacy, controllability, and computer experience to affect employees' security-related behaviors. Based on the results of the examination of the literature, self-efficacy was the dominating variable adopted from social cognitive theory in the information security behavioral studies (Ng et al., 2009; Rhee et al., 2009; Ifinedo, 2014; Ahmad et al., 2019).

2.3.2.7 Neutralization Theory (NT) in Information Security Studies

Neutralization theory was developed in the field of criminology to provide a set of techniques that can explain how individuals can enable themselves psychologically to take actions that break specific rules such as laws, social obligations, and personal beliefs (Sykes and Matza, 1957). Accordingly, the theory suggests a set of techniques that individuals use to neutralize negative thoughts associated with the action and justify performing it. This set of techniques involves denial of responsibility (i.e., justifying the action by removing the responsibility from self), denial of injury (i.e., justifying the action by reducing the harm it may cause in one's own perception), denial of the victim (i.e., justifying the action by blaming the victim of the action as being deserving of it), condemning the condemners (i.e., justifying the action by blaming those who condemn it as doing so out of spite), appealing to higher loyalties (i.e., justifying the action by arguing that such actions are required for the greater good), the metaphor of the ledger (i.e., justifying the action by arguing that they have done so many good things that they should be allowed to do some bad things), and defense of necessity (i.e., justifying the action by arguing that there are no other options other than doing this action) (Sykes and Matza, 1957; Siponen and Vance, 2010; Barlow et al., 2013). The application of one or a combination of these techniques by the individual provides them with the psychological peace and justification to action these behaviors.

In the information security behavioral studies, neutralization techniques were applied as a means for employees to justify performing behaviors that violate the information security policy. Siponen and Vance (2010) found that neutralization techniques affect their intention to violate the information security policy. Similarly, Moody et al. (2018) found that appeal to higher loyalties, metaphor of the ledger, denial of injury, and defense of necessity affect employees' intention to violate information security policy while denial of responsibility and condemning the condemners are insignificant. Barlow et al. (2013) applied only three techniques and found that defense of necessity had an impact on employees' intention to violate information security policy while both denial of injury and metaphor of the ledger were insignificant. Based on the literature, neutralization theory can provide a partial (but not a complete) explanation for employees engaging in unacceptable information security behaviors.

2.3.2.8 Social Bond Theory (SBT) in Information Security Studies

Social bond theory was developed in the criminology field to understand deviant behaviors (Hirschi, 1969). The theory emphasizes the importance of the social element for individuals and states that individuals with stronger social ties will be less likely to perform deviant behavior(s). In explaining these social ties—the social bond—the theory puts forward four key factors. These are attachment (i.e., the individual's sense of respect and interest in his/her social community such as significant others, friends and work colleagues), commitment (i.e., the individual's sense of dedication and devotion toward achieving socially accepted objectives), involvement (i.e., the amount of time the individual spends on conventional social activities), and personal norms (i.e., the individual's values and beliefs about the deviant behavior) (Hirschi, 1969; Cheng et al., 2013; Ifinedo, 2014; Sohrabi Safa et al., 2016).

Three of the information security behavioral studies deployed social bond theory. Two aimed to examine why employees would perform positive behavior (Ifinedo, 2014; Sohrabi Safa et al., 2016), and one observed why they might perform negative behavior (Cheng et al., 2013). Ifinedo (2014) examined the relationship of attachment, commitment, involvement, and personal norms on both attitude and subjective norms in regard to complying with information security policy. He found that commitment, involvement, and personal norms affect employees' attitudes toward complying with information security policy and that attachment and personal norms affect employees' perceived subjective norms. Sohrabi Safa et al. (2016) found that commitment and personal norms affect employees' attitudes toward complying with information security policy while attachments do not have any effect. When it comes to

intention to violate information security policy, Cheng et al. (2013) found that attachment, commitment, involvement, and personal norms affect employees' intention to violate the information security policy.

2.3.2.9 Inconsistent Findings in Information Security Studies

The above review of the main theories used in information security behavioral studies reveals some gaps that are related to the results of concepts adopted from these theories and a deeper review of key concepts has shown that their results are inconsistent. For example, self-efficacy is the most applied concept in the literature; however, its results were not consistent. In the positive security behavioral studies, it was found to have a significant effect on employees' intention to comply with the information security policy in 17 applications (e.g., Boss et al., 2009; Herath and Rao, 2009b; Bulgurcu et al., 2010a; Johnston and Warkentin, 2010; Ifinedo, 2012; Johnston et al., 2015), yet was insignificant in six others (i.e., Pahnila et al., 2013; Ifinedo, 2014; Boss et al., 2015; Bélanger et al., 2017; Menard et al., 2017; Rajab and Eydgahi, 2019). This example applies to most of the identified studies (see Appendix B). However, this literature review could not identify the reasons behind these inconsistencies in the studies. As stated in the research question, this thesis aims to define the BYOD contextual factors which might affect compliance with information security policies. This thesis argues that such inconsistencies in the previous studies might be due to contextual factors such as BYOD-related contextual factors that affected the results of, but were not captured by, these studies.

2.3.3 BYOD in Information Security Studies

The above review of information security literature has shown that many studies have applied different theories to understand, explain, and predict employees' behaviors in regard to (non)compliance with information security policies. These studies have contributed to the body of knowledge and provided many insights and results to help understand the influence of different factors on employees' behavior related to information security. However, only two addressed information security in the BYOD context.

Crossler et al. (2014) investigated the factors behind 360 employees' intentions and behaviors to comply with BYOD-related policies using protection motivation theory. Two unique contexts related to BYOD were investigated: ownership of the devices (user-owned), and sensitivity of the information being processed by and stored on the device. The sensitivity context was examined using the multi-group model to test for the accountant and non-

accountant roles of participants as, arguably, accountants deal with more confidential data, which is more sensitive in comparison to non-accountant roles. The result of their study showed that, for sensitive contexts, perceived threat severity, self-efficacy, and response efficacy had a significant effect on users' behaviors, while perceived threat vulnerability and response cost did not. The same results were reported in the non-sensitive context except for perceived threat severity, which was not significant. Such a result is rational since people, in general, will have a higher perception of the severity of the impact of sensitive information misuse from a non-sensitive context, which may affect how they will act in these two different contexts.

Similarly, Dang-Pham and Pittayachawan (2015) deployed protection motivation theory to investigate users' behaviors related to BYOD information security behaviors, introducing two unique contexts: activity and location. In regard to the activity context, the focus was only on non-work related activities while, for location, both work and home were investigated. Based on the survey data collected from 252 participants, the results for both location contexts were similar: perceived threat severity, self-efficacy, response cost, and rewards were significant in influencing behavior. However, perceived threat vulnerability was only significant in the work location. At first glance, such a result might not appear rational, as people might believe that vulnerability to threat and the probability of breaches is higher at home than at work and so perceived threat vulnerability might be more likely to affect their information security behavior at home. However, we interpret this as a result of the second context that was studied, which is that the type of activity was non-work related: being engaged in non-work activities at work may cause people to be in a higher state of more generalized alertness as they are aware that this may be frowned upon/banned by their employer. Engaging in personal activities at home—in a more relaxed setting—would not prompt the same concerns regarding vulnerability.

As shown above, BYOD introduces different usage scenarios, such as the employee being at work after working hours doing personal activities, being at home doing work-related activities, or other types of scenarios. The two BYOD studies above touched briefly on these usage scenarios by examining whether these contexts affect individuals' behavior. However, neither carried out an extensive review of these contextual factors to determine how they affect individuals' behaviors, and, more precisely, employees' information security-related behavior. In the next section, the thesis presents similar contextual factors in the field of work-life balance and show how they affect individuals' perception of the work and life domains. More

specifically, the next section reviews how ICT affects the work-life domain perception of individuals to build more clarity to answer the research question.

2.4 Work-Life Domain Management Literature

Although the concept of BYOD has only been introduced fairly recently, similar approaches to the impact of information communication technology (ICT) in general have been widely discussed in the work-life domain management literature (e.g., Frissen, 2000; Chesley, 2005; Golden and Geisler, 2007; Heijstra and Rafnsdottir, 2010; Currie and Eveline, 2011; Hislop and Axtell, 2011; Leung, 2011; Sayah, 2013; Cavazotte et al., 2014; Dén-Nagy, 2014). Many studies have postulated that ICT blurs work-life balance while others have gone further, claiming it creates a work-life conflict. On the other hand, others have stated that ICT can be used as a management tool to reach the desired work-life balance. Prior to reviewing these studies, an overview of one of the key theories used in the literature—border theory—and a background of how individuals manage the transition between work domain and life domains is presented.

2.4.1 Border Theory

Border theory is one of the key theories used to explain how people manage the boundaries between life and work (e.g., Clark, 2002; Leung, 2011; Dén-Nagy, 2014). Clark (2000) introduced a new theory about the work/family domain management called work/life border theory. This theory argues that humans are the primary connection between the work and family domains, not emotion. It states that people are border-crossers, as they make transitions from one domain to another (i.e., work to family and vice versa) on a daily basis. These two domains are shaped by people to form borders and determine the relationship of the border-crosser to these domains and their members. In the same manner, people also shape and are shaped by the environment.

The theory aims to explain the interaction between border-crossers and the work-life domain, predict the occurrence of conflict, and provide a framework of how balance can be attained. The theory assumes that work and life are different domains that interfere with each other as they differ in purpose, culture, language, acceptable behaviors, and manner of accomplishing tasks. This makes it easier for some people to cross the boundaries between the two domains and harder for others. Thus, these two domains can be seen as worlds with different rules, thought patterns, and behaviors.

Furthermore, Clark states that the differences between the two domains are classified by valued ends differences and valued means differences. Valued ends refer to the expected goals from each domain, such as attaining an income, a sense of accomplishment, close relationships, or personal happiness. Valued means refer to the ways these goals can be achieved, such as being cheerful, friendly, responsible, capable, honest, loving, or giving. The means through which the desired goals are achieved create cultures that promote certain ways of thinking and behaving, where cultures are a collection of rules that define which means take priority. Although these cultures might not be obvious to employees, they are powerful in shaping behaviors and setting expectations. For example, the cultures in the homes and/or organizations of some employees differ.

In most cases, people are able to manage the two domains through integration and segmentation. Full integration means that the person does not differentiate between what belongs to each, but treats both domains the same—for example when it comes to the person's emotions, related individuals people, and thoughts. In contrast, full segmentation means that each domain is treated differently. However, full integration is not necessarily better than full segmentation and vice versa. Each person will differ in terms of what works best for him/her when it comes to segmentation and integration and people usually change their focus or interpersonal style in order to fit the requirement of the domain they are transitioning to. These changes usually aim to achieve balance, defined as "satisfaction and good functioning at work and at home, with a minimum of role conflict" (Clark, 2000, p.751).

The borders between work and family—and how they are managed by people—should be examined in order to understand how people segment and integrate the two, and at what degree of segmentation or integration a balance can be achieved. Borders can be defined as the demarcation lines between the work and family domains that define where one of the domains starts or ends. Three main forms of borders have been identified in the literature: 1) physical, 2) temporal, and 3) psychological. Physical borders refer to locations or spaces, such as home or work building, which give the individuals a sense of which domain they are in. Temporal borders refer to the time that defines the domain, such as working hours. Psychological borders refer to the rules that individuals set for themselves to define which emotions, patterns of thinking, or behaviors are appropriate for each domain. Individuals usually self-regulate their psychological borders, and in doing so, they usually use temporal and physical borders.

In addition, border theory defines permeability as a border characteristic. Permeability is defined as the degree to which elements of one domain enter into the other and permeations can be physical, temporal, or even psychological. An example of physical and temporal permeations is a person who is working from home after working hours, where the setup of the office resembles the workplace office, and family members keep on interrupting him or her. An example of psychological permeation is when a person takes his or her negative emotion from work to home or vice versa.

Flexibility is another characteristic of borders according to border theory. Flexibility refers to the extent that a border can expand based on the demands within each border. Individuals that are free to work from any location and at any time have a higher degree of flexibility for physical and temporal borders. In the same manner, individuals that are able to think about work at home and about home at work have a higher degree of psychological flexibility.

When both permeability and flexibility are high, the areas around the borders between work and family are no longer exclusive to either of the two domains; a 'borderland' is created that merges the two domains. This phenomenon is referred to in border theory as blending. When the two domains are too different, it may cause negative impacts on individuals who experience conflicting demands from each domain, affecting their sense of identity and purpose and potentially resulting in schizophrenia. However, when the two domains are similar, in some cases, blending can lead to better integration and a sense of wholeness.

Clark (2002) states that there are two different kinds of border-crossers: central participants and peripheral participants. Central participants have influence and identification, while peripheral participants do not. Influence refers to participants' competence required by the domain and is affiliated with domain members internalizing the values and culture of the domain. Identification refers to "individuals [who] find meaning in their responsibilities and find that their responsibilities mesh with their self-concept" (Clark, 2000, p.760).

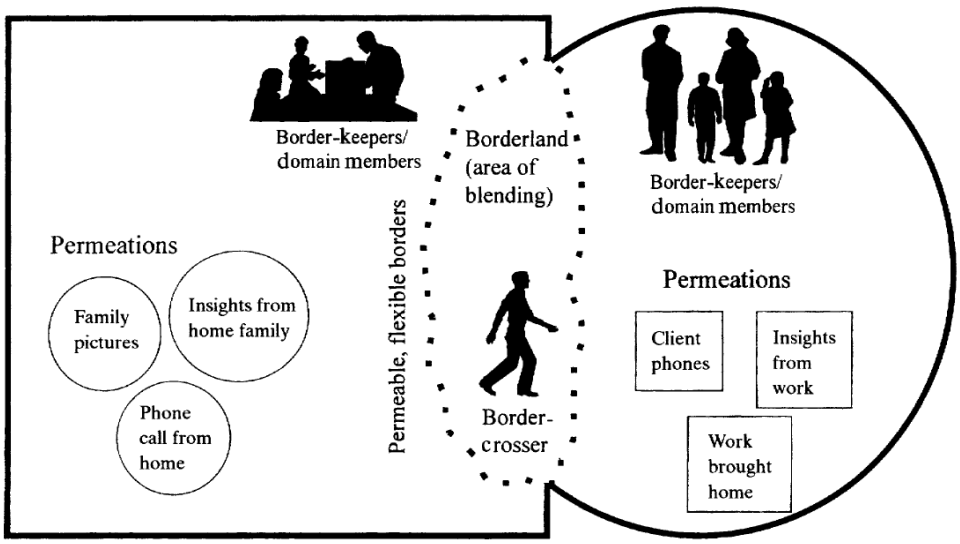
In addition to border-crossers, Clark defines two additional actors when it comes to borders: domain members and border-keepers. Domain members are members in each domain who affect how border-crossers define domains and borders. When domain members become influential in how border-crossers define domains and borders, they are referred to as border-keepers. Both domain members and border-keepers impact how border-crossers manage

borders; however, border-keepers are more influential. Examples of typical border-keepers are supervisors (at work) and spouses (at home).

Domain members and border-keepers have two key attributes: other-domain awareness and commitment to the border-crosser. Other-domain awareness refers to how much domain members and border-keepers of a certain domain are aware of the border-crosser's obligations in the other domain. Commitment to the border-crosser refers to "[c]ommitment [that] is manifested by caring about the border-crosser as a total person, not just in terms of how the border-crosser fills one's immediate needs. Commitment is manifested when domain members support the border-crossers in their other domain responsibilities" (Clark, 2000, p.763).

Clark (2002) conducted a study to understand how individuals create balance between work and family through enacting their work and home environments. Enactment refers to the process individuals follow to organize, make sense of, and create possibilities for action with their external environment. Clark argues that individuals can create a work/family balance by performing across-the-border communications where individuals (i.e., border-crossers) communicate about their work with their family and about their family with their colleagues at work. In order to conduct the study, Clark examined qualitative data from 15 interviews and two focus groups and identified three themes of communication. From a lower to a higher level of information richness, they are: 1) communication as an obligation; 2) communication as a center of activities; and, 3) communication as an understood, meaningful experience. Based on this, Clark then conducted a quantitative study: she developed a questionnaire and collected usable data from a sample of 179 individuals. The result showed that cross-border communications vary depending on the flexibility and permeability of the work and home borders. Some themes of cross-border communications can contribute to a better work-family balance, where work-family balance reflects a higher satisfaction with work and family, better functioning with work and family, and lower role conflict (Clark, 2002).

The summary of border theory provided by Clark (2000, p.754) is shown in Figure 4. The theory provides a good lens to examine and understand how employees make sense of their life and work domains and manage the borders between the two. BYOD can affect the physical, temporal, and psychological borders, making it difficult to manage these borders and can lead to the blending of the two domains which creates gray areas when making decisions in regard to compliant behaviors related to information security.



Domains	**Borders**
extent of segmentation and integration overlap of valued means and ends overlap of cultures	border strength permeability flexibility blending
Border-crossers	**Border-keepers & other domain members**
peripheral vs. central domain membership identification influence	other-domain awareness commitment to border-crossers

FIGURE 4: BORDER THEORY

(CLARK, 2000, P.754)

2.4.2 ICT Effect in Work-life Domain Management Literature

ICT (and more specifically, the usage of mobile phones) has been shown to blur the boundaries between the work and life domains, which in turn affects work-life balance. Chesley (2005) conducted a quantitative analysis to study the impact of ICT on family satisfaction, anxieties, and distress. Using spillover theory, which posits that workers carry their feelings, attitudes, skills and behaviors with them from work to life or from life to work, Chesley analyzed longitudinal data (N = 1,367) from the Cornell Couples and Careers Study, showing that employees blur work/family boundaries due to the usage of technology, which results in negative consequences. Her results showed that the usage of cell phones led to an increase in the level of spillover from work to family and this had a negative impact, increasing employees' distress and lowering family satisfaction.

Further, when it comes to family to work spillover, the result showed that only women had a negative spillover, indicating that genders differ when it comes to how they deal with work/family boundaries. Hislop and Axtell (2011) conducted research focusing on how non-managerial engineers manage their work/non-work boundary during working hours using mobile phones. Three case studies on different organizations were conducted with a total of 17 interviewees. None of the participants faced any issues after working hours; however, the boundaries between work/non-work during working hours were blurry. For example, they used their phones as a method to manage their work/non-work boundary. However, each person used mobile technology differently, in different situations, and at different times to manage the boundary. Further, the result showed that people could not be characterized purely as 'segmentors' or 'integrators' as they can be either depending on the domain, time, or people they are with.

Leung (2011) also showed how ICT could affect work-life balance by creating a work-life conflict which has a negative impact. Using data collected from 612 office workers in Hong Kong through telephone surveys, Leung employed both border theory and spillover theory to examine the impact of ICT connectedness on negative spillover from work to home and from home to work via increased permeability and flexibility and to ascertain how the spillover affects job burnout and job/life satisfaction. The main result of the analysis shows that ICT can influence the blurriness of work-life boundaries, which might have a positive and/or negative effect on working people where ICT connectedness has an impact on the permeability of the work and family domains. Further, ICT connectedness also impacts the flexibility of the work and life domains, where workers perceive that the more connected they are to ICT, the fewer conflicts they will have between work and family. The flexibility of the work and home domains affects people's perception of home/life boundaries' permeability. An increase in boundaries' permeability at home leads to a negative spillover from work to home. Also, increasing flexibility at home leads to a negative spillover from work to home, while increasing flexibility at work will decrease the negative spillover from work to home. Job burnout was found to be directly affected by the negative spillover that people experienced and has been found to affect job satisfaction but not necessarily home satisfaction. Only job dissatisfaction (not job satisfaction) was found to be associated with negative spillover from work to home and from home to work. In summary, Leung's study shows job satisfaction is usually reported by older people—who feel that the internet can help them achieve their work-related tasks, that traditional media helps them to relax after work, and that the impermeable home border protects

them from work entering their home domain. On the other hand, low job satisfaction was associated with negative spillover into home from work, leading to job burnout, particularly in young females with mobile access that have high permeable boundaries and low flexibility at work.

This stream of negative impacts of ICT on work-life balance is supported by other studies' findings. Cavazotte et al. (2014) conducted a series of interviews to investigate the effect of company-owned smartphones on employees' lives. They argue that the usage of smartphones provides employees with increased speed, accessibility, and accuracy, leading to a better sense of autonomy and flexibility. However, smartphones also have a negative impact on the personal domain of employees, as they can tap into new places, time slots, and social contexts that intensify the workload. As a result, employees use self-justifications to justify the increased escalation in communication. Self-justification refers to the critical reflections and narrative strategies applied by employees to the usage of smartphones for work purposes. Cavazotte et al. recorded three narrative strategies: 1) employees justify that they have more control over engaging in more communication; 2) employees dis-identify with the role they play (i.e., the usage of irony or jokes to maintain the idea that they are autonomous from management ideology, while carrying out all of the work instructed by the organization); and, 3) the situation is out of their hands, and there is no escaping it.

In the same way, Currie and Eveline (2011) show the impact of e-technology on the work-life balance of academics. They argue that, due to e-technology allowing academics to perform work at any place and time, work has been transferred to their home lives and has affected their work-life balance. They conducted their study on academics who had young children, where a three-stage process was used to collect the data: an online survey was followed by interviews with a smaller sample of the survey respondents who also kept a time diary. The result of their study showed that having e-technology at home was beneficial for their work but came at a cost to their family, as there was a majority of dissatisfaction with work-life integration.

Heijstra and Rafnsdottir (2010) conducted 20 in-depth interviews in Iceland, targeting academics, to examine whether ICT supports their work-life balance. The study showed that academics find it more difficult to disengage themselves from work. ICT can support the flexibility of domains and gives academics the freedom to choose the location of work and time spent working, but the perception that they needed to be available all the time and unable to disengage from work was found to increase work/family conflict and the risk of burnout.

Additionally, Diaz et al. (2012) conducted quantitative research to study the relationship between communication technology flexibility, communication technology, work-life conflict, and work satisfaction, collecting and analyzing data from 193 employees. The study showed that communication technology flexibility had a positive impact on increasing communication technology use. Similarly, increased usage of communication technology led to an increase in both work satisfaction and work-life conflict, the latter having a negative effect on the former. Frissen (2000) employed a qualitative case study to examine whether ICT can provide a solution to the increasing work-related demands on households in the Netherlands. She found that ICT was not perceived as a solution; however, it is being used to solve these problems. Tenakoon (2007) performed a qualitative study that showed a similar negative effect of ICT on work-life balance; the results showed that mobile phones are one of the main types of ICT that affect family-to-life spillover.

On the other hand, other studies have aimed to show that ICT and, more precisely, mobile phones can be used as a means to manage the two domains and achieve balance. Golden and Geisler (2007) conducted a qualitative study to examine the effect of Personal Digital Assistants (PDAs) as a work/personal life boundary management tool. The study interviewed 42 PDA users from the USA, and the results showed that users interpret PDA usage as a method of controlling the work-life boundary. This control occurs through the integration and segmentation of work life and personal life. Further, users manage the work-life boundaries' flexibility and permeability in both directions. This study can be seen as an example of how ICT, although restricted to one type of device, can provide better control for individuals over work-life boundaries and create the desired balance.

Hubers et al. (2011) conducted quantitative research in order to examine the impact of ICT on different coping strategies adopted by households in the Netherlands. They analyzed data from 525 people living with partners, where the sample included single and dual-earner householders. The focus of this analysis was to determine who adopted ICT-enabled strategies and whether ICT usage complements or substitutes for other coping strategies. They found that ICT-related strategies are frequently used by highly-educated employed parents to complement other work-life balance strategies to achieve an overall work-life balance. The usage of ICT and the choices people make depend on many factors and conditions, such as the presence of young children, employment factors (occupational level and sector), ICT possession, affordability, skills, and spatial accommodations (characteristics of the home and workplace

environments). An earlier study by Christensen (2009) conducted a qualitative review on the usage of mobile phones by families in Denmark, in which 17 semi-structured interviews with nine families were conducted. The focus of the analysis was on the parents, their communication with their children, and with each other. The results showed that parents and children use mobile phones to mediate by creating a feeling of closeness when they are physically separated.

Sayah's (2013) qualitative study showed that multiple ICT-mediated tactics are used by individuals to manage work-life boundaries. Individuals have different preferences when it comes to managing boundary dimensions (i.e., temporal, spatial, or psychological) and boundary permeability direction (i.e., work to life or life to work); therefore, they cannot be classified as only 'integrators' or only 'segmentors.'

Based on the above literature review, it is clear that ICT and the increased usage of mobile phones, whether personally-owned or provided by organizations, can cause the boundaries of these two domains to be blurred. ICT has been identified as a way to manage work and life boundaries yet, at the same time, it can also be the cause of conflict between the two domains. Thus, this effect will have widespread impacts on how employees behave in different situations. More specifically, this thesis is interested in situations caused by the perception of work/life domain brought about by BYOD and how they affect their information security-related behaviors.

2.5 A Critical Review of Existing Literature

This section aims to summarize the research gaps revealed by the comprehensive review in the previous sections. Two critical gaps have been identified, which this thesis will aim to address. The first relates to the low numbers of BYOD studies identified in the behavioral studies in information security literature and, consequently, the limited theoretical perspective used to examine the BYOD and the inconsistent results from the protection motivation theory variables in the literature. The second gap is related to the limited examination of the effect of BYOD on work-life domain perception and the effect of work-life domain perception on information security-related behaviors.

2.5.1 Limited Research on BYOD in Information Security Literature

The literature review revealed that many studies have applied different theories in order to investigate information security behaviors (e.g., Boss et al., 2009; Herath and Rao, 2009a;

Bulgurcu et al., 2010a; Siponen et al., 2010; Ifinedo, 2012; Pahnila et al., 2013; Yoon and Kim, 2013; Johnston et al., 2015). However, only two were identified which extended the information security behaviors' examination to the BYOD application (i.e., Crossler et al., 2014; Dang and Pittayachawan, 2015). The majority mostly focused on general information security behaviors that occur in the organizational setting (e.g., Pahnila et al., 2007a; Siponen et al., 2007; Herath and Rao, 2009a; Zhang et al., 2009a; Bulgurcu et al., 2010a; Hu et al., 2012; Ifinedo, 2012; Al-Omari et al., 2013; Yoon and Kim, 2013), examining different theories and variables in standard organizational settings when employees use organization-provided devices.

The literature review discussed how BYOD is becoming more of a norm rather than an exception (e.g., Crossler et al., 2014) and more employees are/will start using their personally-owned devices that have access to their organization's information assets. The review also showed that BYOD has its own specific challenges related to information security that may cause harm to the organizations (e.g., Disterer and Kleiner, 2013; Garba et al., 2017). Since humans are considered the weakest link in information security (e.g., Bulgurcu et al., 2010a; Dong et al., 2010; Caldwell, 2012), this thesis argues that there is a need to explore further and study the effect of adoption of BYOD on employees' behavior regarding information security.

Information security research, in general, has employed different theories and concepts to better understand the information security behavior performed by employees in an organizational context. As a result, there is a richer understanding of how different variables adopted from these theories affect employees' behaviors. The summary of these results (see Appendix B) shows how these different variables were examined in the information security literature. However, most of these studies focused on the traditional usage of technology in relation to information security and employees' behaviors. As technology evolves, new trends and approaches are introduced that may affect current information security policies and the current intervention programs aimed at increasing employees' compliance with these policies.

Because of the lack of BYOD studies in the information security behavioral field we still lack in-depth knowledge of this phenomenon. In the only two studies on contextual factors relevant to BYOD (i.e., Crossler et al., 2014; Dang and Pittayachawan, 2015), only protection motivation theory was applied and tested, leaving room for opportunities to include and test other theoretical perspectives. The application of other theories will provide a richer understanding of information security behavior in employees adopting BYOD.

Furthermore, inconsistent results from the protection motivation theory application in BYOD studies have been identified. Perceived threat vulnerability, one of the key variables in PMT, had a significant positive effect on employees' intention to comply with information security policy in most studies (e.g., Siponen et al., 2006; Ifinedo, 2012; Pahnila et al., 2013; Siponen et al., 2014; Sommestad et al., 2015; Warkentin et al., 2016; Rajab and Eydgahi, 2019) yet in others this relationship was shown to be insignificant (e.g., Vance et al., 2012; Pahnila et al., 2013; Boss et al., 2015; Johnston et al., 2015; Menard et al., 2017). Similarly, self-efficacy had a significant positive effect on employees' intent to comply with information security policy in many studies (e.g., Siponen et al., 2006; Pahnila et al., 2007b; Siponen et al., 2007; Boss et al., 2009; Herath and Rao, 2009b; Bulgurcu et al., 2010a; Johnston and Warkentin, 2010; Siponen et al., 2010; Son, 2011; Ifinedo, 2012; Vance et al., 2012; Al-Omari et al., 2013; Siponen et al., 2014; Johnston et al., 2015; Rocha Flores and Ekstedt, 2016; Warkentin et al., 2016; Yoo et al., 2018) but was found to be insignificant in others (e.g., Pahnila et al., 2013; Ifinedo, 2014; Boss et al., 2015; Bélanger et al., 2017; Menard et al., 2017; Rajab and Eydgahi, 2019). On the other hand, reward had a negative significant effect on employees' intention to comply with information security policy in some studies (e.g., Vance et al., 2012) while no significant relationship was identified in others (e.g., Siponen et al., 2014; Posey et al., 2015). The relationship of response efficacy with employees' intent to comply with information security policy was found to be positive (e.g., Siponen et al., 2006), negative (e.g., Vance et al., 2012), and insignificant (e.g., Pahnila et al., 2007b; Siponen et al., 2010; Siponen et al., 2014; Boss et al., 2015; Warkentin et al., 2016).

Similar outcomes were found in the two information security behavioral research studies that examined contextual factors relevant to BYOD. When using their own devices in work locations, the perceived threat vulnerability relationship with employees' intention to comply with information security policy was found to be significant in one study (Dang and Pittayachawan, 2015) but not in the other (Crossler et al., 2014). Likewise, response cost had a significant effect on employees' intention to comply with information security policy in one (Dang and Pittayachawan, 2015) but not the other (Crossler et al., 2014).

This widespread inconsistency of results suggests that the effect of PMT in information security behavior literature is yet to be fully understood, both in general information security behavioral studies and those that focus on BYOD. PMT can be further examined to understand the discrepancy in the results reported by the previous studies for the different variables included

in PMT with relation to employees' intention to comply with information security policy and in the context of BYOD.

It is critical to continue to review prior studies in light of new technologies. The advances in technology are neverending and with each comes a new perspective through which these studies can be reexamined. This is one of the gaps that this thesis is aiming to fill with its examination of BYOD as a new technological practice.

2.5.2 Limited Research on Work-Life Domain Perception in Information Security Studies

It is now common for employees to bring their personally-owned devices to work, and use them to do both work-related and personal activities. The usage of ICT in a similar manner has been shown to affect employees' work-life domain management, where some employees use it to manage the border between life domain and work domain, whether these borders are physical, temporal, or spatial. The above review suggests that the work-life domain management literature has shed some light on the impact of ICT on blurring the border between the work and life domains (e.g., Chesley, 2005; Leung, 2011). Life and work borders (i.e., physical, temporal, and psychological borders) have been shown to blend into grey areas as a result of ICT by some studies and to be managed by ICT by others (e.g., Chesley, 2005; Leung, 2011; Cavazotte et al., 2014). However, no single study was identified which put forward a comprehensive framework that captured the complexity of BYOD and defined related contextual factors that influence employees' interpretation of BYOD as a life or work domain.

Furthermore, the unique context of BYOD, which leads to different usage scenarios by employees, which in turn affects their interpretation of making sense of their home or work domains, was not investigated in relation to information security behaviors. Employees' inability to definitely categorize work or life domains creates a gray area which affects their information security behaviors. In such situations, employees might be influenced in their behaviors by different factors.

The vast majority of information security-related behavior literature, as presented in the literature review, focused mainly on the work environment context. Such a traditional view of employees only working in offices and using organization-provided devices is less relevant in today's world. It did not examine how different work arrangements or usage of different technologies may affect the current understanding of information security behaviors and factors

affecting these behaviors. This thesis will focus on addressing this gap with the focus on BYOD usage from the work-life domain perspective.

2.6 Chapter Summary

This chapter presents a comprehensive review of the theoretical perspectives from both information security literature and work-life domain literature, and critically examines the existing literature to identify the key research gaps that drive this thesis. First, an overview of information security is discussed to show how it is an integral part of each organization and the efforts made by these organizations to protect their information assets. People have been identified as the weakest link in information security and, as a result, organizations have put in place information security policies and intervention programs to direct their employees' behaviors to reduce risks to their assets.

Then, a thorough literature review of existing information security research was conducted to examine the theories explaining employees' information security-related behavior in general and BYOD in particular. Although bring your own device has become the norm, only two studies on contextual aspects of its effect on employees' information security-related behaviors were identified. Furthermore, the results across these studies were not consistent as many factors, mostly adopted from protection motivation theory, have been shown to affect employees' information security-related behaviors in one but not in the other study. In addition, the effect of how bring your own device influences employees' perception of which domain they are in – work or life – and how this perception affects their information security-related behavior was not identified as being examined in any study.

Since BYOD has been shown to affect employees' work-life domain management, literature on work-life domain management was also reviewed to examine how it could shed light on BYOD research. The review suggests that existing research on work-life domain needs to be updated to take into account new technological developments to examine how ICT usage, in this case, BYOD, shapes perceptions of work-life domains. Furthermore, little research has been conducted to examine how such perceptions of work-life domains could affect security compliance behavior in particular.

CHAPTER THREE: THEORETICAL DEVELOPMENT AND RESEARCH MODELS

The review of the literature revealed key gaps involving the effects of BYOD on employees' information security-related behaviors. Only two studies were identified that had tested information security-related behaviors in the context of BYOD, and neither provided a comprehensive and updated view of the BYOD contextual factors in relation to information security-related behaviors. This research argues that making sense of BYOD usage scenarios from the work-life domain perspective will not only provide a comprehensive understanding of the BYOD phenomenon, but also shed light on the inconsistent results in prior research on information security compliance.

This chapter therefore develops a research model explaining the BYOD contextual factors shaping employees' perception of the work-life domain; and then a research model to examine how employees' perceptions of the work-life domain could alter their information security policy compliance behaviors. The first step defines and tests the contextual factors of BYOD to understand their influences on employees' interpretations of BYOD and their perceptions of whether they are in the life domain or work domain. The second step examines the effect of employees' perception of which domain they are in on their compliance with the information security policy, examining the usability of this new approach and the necessity of re-investigating information security to incorporate the work-life domain perspective.

3.1 BYOD Contextual Factors and Work-Life Perception

Many employees today can use their personal devices to perform both personal and work-related activities. These devices can be used at any time and anywhere to process sensitive personal and work-related information. Owing to the unique characteristics of BYOD, employees can adopt different usage scenarios, which are interpreted differently by different employees. Employees' interpretations of BYOD usage scenarios can thus affect their perceptions of whether they are in their work or life domain, even creating a gray area between the two.

To define these contextual factors, prior research on the work-life domain was reviewed. Existing research on the work-life domain shows that employees use a set of boundaries (e.g., temporal, physical, social, behavioral, and psychological) to separate their life and work domains (e.g., Ashforth et al., 2000; Clark, 2000; Olson-Buchanan and Boswell, 2006; Park

and Jex, 2011; Fonner and Stache, 2012). These studies illustrate how employees manage their transition between the work and life domains by crossing boundaries. For example, an employee may transition from his/her work domain to his/her life domain by crossing one or more of the following: temporal boundary (e.g., end of working hours), physical boundary (e.g., leaving the work location), social boundary (e.g., saying goodbye to coworkers), behavioral boundary (e.g., submitting the last work task of the day), and psychological boundary (e.g., a sense that they are away from work). Building on these studies, five contextual factors are proposed: device ownership, location, time, activity, and data sensitivity, as shown in Table 3.

TABLE 3: BYOD CONTEXTUAL FACTORS

Device Ownership	Employees use their personal devices (e.g., smartphone, laptop, tablet) rather than devices owned by their organization.	Employees use the organization's devices (e.g., workstation, smartphone, laptop, tablet).
Employee Location	Employees use the devices in a non-work environment (e.g., home, coffee shops, hotels).	Employees use the devices on the organization's premises (e.g., office, meeting rooms, other branches).
Time of Activity	Employees use the devices during non-working hours.	Employees use the devices during working hours.
Activity Type	Employees use the devices to work on personal tasks (e.g., social media, personal emails, reading news, browsing the internet).	Employees use the devices to perform work-related tasks (e.g., developing reports, processing transactions, responding to work emails).
Data Sensitivity	Employees use the devices to process non-sensitive personal or organization information (i.e., either accessed remotely or stored on the device).	Employees use the devices to process sensitive personal or organization information (i.e., either accessed remotely or stored on the device).

3.1.1 Device Ownership

ICT has been shown to affect employees' work-life domain management (e.g., Frissen, 2000; Chesley, 2005; Golden and Geisler, 2007; Heijstra and Rafnsdottir, 2010; Currie and Eveline, 2011; Hislop and Axtell, 2011; Hubers et al., 2011; Leung, 2011; Sayah, 2013; Cavazotte et al., 2014; Dén-Nagy, 2014). In some cases, ICT and the usage of mobile phones have been shown to blur the work-life balance (Chesley, 2005; Hislop and Axtell, 2011; Leung, 2011), while in others, ICT devices have been used to manage the integration and segmentation of the work-life domain. Individuals may thus use multiple devices to create a boundary between their work and life domains (Fleck et al., 2015).

This study argues that the actual ownership of the device can affect employees' perceptions of whether they are in their work or life domain. This perception can be affected by whether individuals feel they have crossed a psychological boundary between the domains; different individuals view the integration and segmentation of the two domains in different ways (Clark, 2000; Dén-Nagy, 2014). Therefore, while one individual might perceive their state to be in the work domain or in the life domain depending on the device ownership, another individual might be unable to segregate the two, resulting in a blurry state. Cavazotte et al. (2014) claimed that company-owned smartphones used by employees had a negative effect on the life domain. Additionally, Duxbury et al. (2014) showed that, based on the different boundary management strategies adopted by individuals, the usage of a company-owned smartphone can lead to a struggle to segment the life domain from the work domain, or it can be used as a boundary management tool. Similarly, the usage of an individual's personal device in the work environment may affect his/her ability to segment the work domain from the life domain. Device ownership, as a contextual factor, is foundational in BYOD because it differentiates the traditional employee usage of ICT devices that are owned by the organization from the relatively new practice of using an employee-owned ICT device. Accordingly, the first BYOD contextual factor that this study puts forward relates to whether the device is owned by the employee or the organization. This study thus posits the following:

***H1**: Device ownership (i.e., whether owned by the employee or the organization) impacts employees' perceptions of whether they are in the life or work domain.*

3.1.2 Employee's Location

The second BYOD contextual factor this study proposes relates to location. This contextual factor relates to the spatial boundary between the life and work domains (Ashforth et al., 2000; Clark, 2000). With BYOD, individuals can work from anywhere due to the flexibility ICT enables. Duxbury et al. (2014) show that one of the boundaries that individuals may use to manage the integration or segmentation of their work and life domains is physical location. It can act as a domain border that individuals use to make sense of which domain they perceive themselves to be in (Clark, 2000). For example, an employee who is still in the workplace will tend to perceive that s/he is in the work domain, while an employee who is in the living room of his/her home will tend to perceive that s/he is in the life domain. Therefore, the second hypothesis in this study is posited as follows:

H2*: An employee's location while using the device (i.e., using the device at home vs. using the device in the workplace) impacts the employee's perceptions of whether they are in the life or work domain.*

3.1.3 Time of Activity

With the wide application of internet technologies and mobile devices, 'working time' has experienced a great change (Fonner and Stache, 2012). For instance, telecommuting permits employees to work from any location, eliminating or reducing long commute times in heavily populated areas while zero-hour contracts pay workers only for those hours worked and have no minimum hour guarantees. In such cases, employees have more flexibility to determine their working time, which is not necessarily the same as the working time defined by their organizations. However, the widespread adoption of smartphones has also created an expectation that employees will both be available and will perform work-related activities outside of their contracted working hours (Dén-Nagy, 2014; Garba et al., 2015). These changes allow employees to enjoy more autonomy or flexibility with their working time, and employees thus tend to be more proactive in distinguishing between their working and non-working times (Ylijoki, 2013). As a result, the temporal boundary is one of the boundaries that people cross to determine whether they are in the work or the life domain (Ashforth et al., 2000; Clark, 2000). This flexibility of being connected all the time is also applicable to BYOD, where employees can use their own devices at any time, whether during or after working hours. Therefore, time is defined as the third BYOD contextual factor. The study puts forward the following hypothesis:

***H3**: Time of device usage by the employee (i.e., using the device outside normal working hours vs. using the device during normal working hours) impacts employees' perceptions of whether they are in the life or work domain.*

3.1.4 Activity Type

With personal devices, employees may perform either personal or work-related activities. When performing work-related activities, an employee might have a higher level of awareness of organizational restrictions (e.g., rules, procedures, access rights, and other security controls); however, such regulations may not be relevant when employees are performing personal tasks (Li and Siponen, 2011). Park et al. (2011) stated that a behavioral boundary is needed to manage the segmentation and integration of the work and life domains. In the same manner, BYOD allows the usage of personally-owned devices for different types of tasks. The type of task—whether work-related or personal—will affect the individual's perception of whether they are in the work or life domain. As a result, this study posits the following hypothesis:

***H4**: The type of activity performed by the employee (i.e., personal-related activity vs. work-related activity) impacts employees' perceptions of whether they are in the life or work domain.*

3.1.5 Data Sensitivity

The sensitivity of the information that employees are processing or storing on their devices also affects their perceptions of the work-life domains. In relation to BYOD, the reference here is to the type of information stored on or processed by the device, whether personal or work-related information. Therefore, the sensitivity of these data may also trigger psychological ownership because people experience a sense of relation to different objects—physical or nonphysical—which occurs when they feel that they own the object (Anderson and Agarwal, 2010). The psychological boundary is also discussed in the work-life literature (Clark, 2000). Accordingly, data sensitivity is proposed as one of the contextual factors of BYOD that applies to two data sets, one owned by the company and the other owned by the employee. As such, this study posits the following hypotheses:

***H5a**: Employees' perceptions of the sensitivity of organization-owned data processed on the device (i.e., non-sensitive organization data vs. sensitive organization data) impacts employees' perceptions of whether they are in the life or work domain.*

***H5b**: Employees' perceptions of the sensitivity of personally-owned data processed on the device (i.e., sensitive personal data vs. non-sensitive personal data) impacts employees' perceptions of whether they are in the life or work domain.*

3.1.6 Research Model 1

Following the previous hypotheses and drawing from the literature on work-life boundaries, this research argues that employees make sense of whether they are in the life or work domain through their interpretations of different BYOD usage scenarios, based on their work-life segregation and integration strategies. Specifically, those who rely on temporal distance to separate the two domains tend to give more weight to time when making sense of the BYOD usage scenario, while those who usually rely on physical location for work-life segregation might be more sensitive to place than to the other contextual factors. Thus, employees rely on contextual factors—namely, device ownership, employees' location, time of activity, activity type, and data sensitivity—to make sense of whether the BYOD usage scenarios come under the work or life domain and this sense-making relates to employees' work-life segregation strategies.

Accordingly, Figure 5 shows the research model that was developed to achieve the first aim of this study. The model relates to an understanding of the impact of BYOD contextual factors on employees' interpretations of being in the work or life domain. In addition to the above hypotheses, this study adopts a set of controls from existing studies in relation to gender (Park and Jex, 2011; Berkowsky, 2013; Xie et al., 2018), age (Berkowsky, 2013; Xie et al., 2018), marital status (Park and Jex, 2011; Berkowsky, 2013; Xie et al., 2018), education (Berkowsky, 2013), experience (Johnston et al., 2015), position (Berkowsky, 2013), organization size (Bulgurcu et al., 2010a), industry (Bulgurcu et al., 2010a), job role (Herath and Rao, 2009b), tenure (Son, 2011), and IT knowledge (Bulgurcu et al., 2010a).

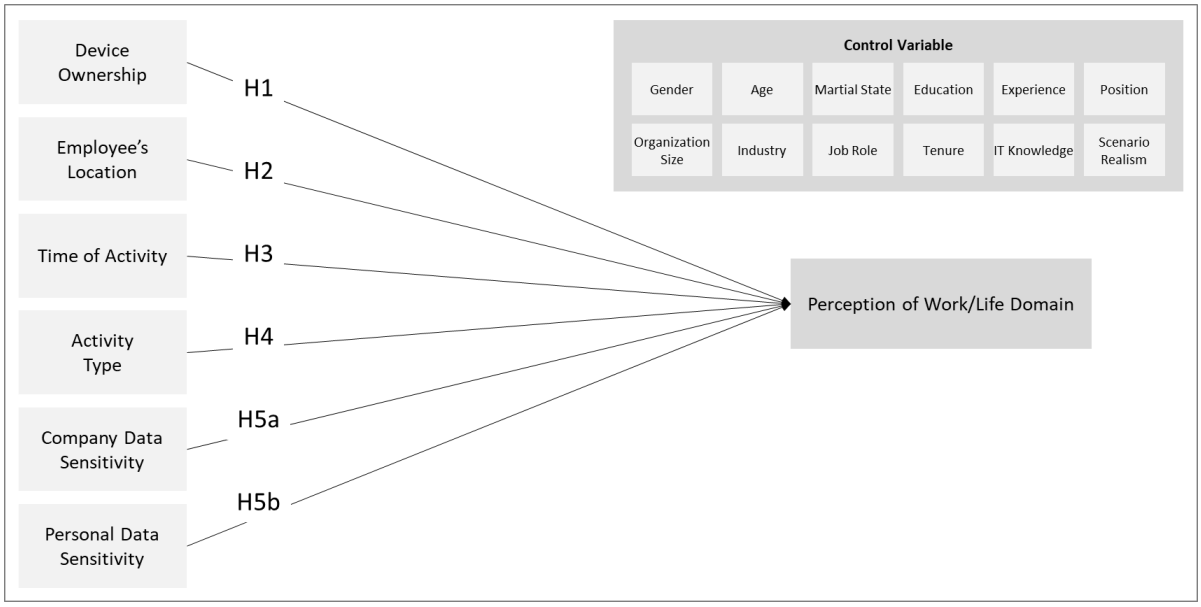


FIGURE 5: RESEARCH MODEL 1

EFFECT OF BYOD CONTEXTUAL FACTORS ON EMPLOYEES' PERCEPTION OF WORK-LIFE DOMAIN

In this section, the thesis defined its first research model, which explains how BYOD contextual factors affect employees' perception of the life domain or the work domain. This thesis posits that employees' perception of life and work domains affects their information security-related behaviors. Therefore, the second model in the next section will study how employees' information security behaviors are affected by their perception of life and work domain.

3.2 The Impact of Work-Life Domain Perception on Information Security Policy Compliance

As stated in the introduction to this chapter, the second step of this research aims to understand the impact of employees' perceptions of the work-life domain on their information security compliance behaviors. Accordingly, a research model is developed to examine this impact, based on protection motivation theory (PMT) which was illustrated in the literature review in Chapter 2 to be the most dominant theory used in similar studies. This section first defines the dependent variable (i.e., intention to comply with the information security policy) and then discusses the relationship between the PMT variables and the dependent variable. Related hypotheses will also be presented.

3.2.1 Dependent Variable: Intention to Comply with Information Security Policy

The dependent variable in the second proposed research model is the intention to comply with the information security policy. Although it would be more accurate to measure the actual behavior, doing so has been deemed too difficult, and most studies have thus measured intention rather than actual compliance behaviors (e.g., Herath and Rao, 2009b; Bulgurcu et al., 2010a; Johnston and Warkentin, 2010; Warkentin et al., 2011; Ifinedo, 2012; Vance et al., 2012; Dang and Pittayachawan, 2015). The difficulties manifest in the measurement of compliancy behaviors, where asking participants to self-report their actual compliance might not produce accurate responses due to fear of exposing nonconforming behaviors.

To overcome this challenge, information security studies have mostly adopted intention because it has been proven in the existing literature to be one of the most significant predictors of behavior. According to the theory of reasoned action (Fishbein and Ajzen, 1975; Ajzen, 1991; Fishbein, 2000; Fishbein and Ajzen, 2010), individuals perform behaviors when they have an intention to perform those behaviors. This relationship has been tested in many disciplines and has shown its validity. This finding is illustrated in a meta-analysis conducted by Armitage and Conner (2001), which revealed a mean correlation of 0.47 between intention and behavior among 48 studies examined. Similarly, Notani (1998) conducted a meta-analysis of 45 studies and found an average correlation of 0.41 between intention and behavior. Another meta-analysis of 98 studies found an average correlation between intention and behavior of 0.45 (Randall and Wolff, 1994) while Sheppard et al.'s (1988) meta-analysis of 87 studies found a correlation of 0.53 between intention and behavior. These meta-analyses covered behaviors in many domains including drug and alcohol usage, recycling, political behaviors, smoking, public transportation usage, condom usage, and food and beverage-related behaviors. As the results of these meta-analyses demonstrate, the correlation between intention and behaviors ranged from 0.41 to 0.53, thus suggesting with a level of confidence that if an individual forms the intention to perform a behavior, the probability of performing that behavior is very high.

This support of intention as a predictor of actual behaviors provides more confidence in its use as the dependent variable. Such practice, as discussed, is common across existing information security studies. Therefore, this research uses intention—the intention of employees to comply with the organization's information security policy—as the dependent variable.

3.2.2 Independent Variables: Protection Motivation Theory

As presented in the literature review, PMT is one of the most widely applied theories explaining employees' compliance behaviors relating to the information security policy in their organizations (e.g., Boss et al., 2009; Herath and Rao, 2009b; Herath and Rao, 2009a; Bulgurcu et al., 2010a; Johnston and Warkentin, 2010; Siponen et al., 2010; Ifinedo, 2012; Johnston et al., 2015). It was also used in the two BYOD studies that investigated security-related behaviors (Crossler et al., 2014; Dang and Pittayachawan, 2015). Accordingly, PMT was adopted for this research due to its capacity to explain protection-related behaviors (i.e., information security policy compliance). Based on PMT, this study proposes a research model to test the impact of employees' perceptions of the work-life domain on their information security compliance behaviors and examines how work-life domain perception shaped by BYOD could affect the relationship between PMT variables and intention to comply with information security policy.

According to PMT, employees' intention to comply with information security policy is influenced by an assessment of the consequences of non-compliance as well as the individual's capability to comply. Three variables capture the employees' assessment of the consequences of non-compliance (i.e., threat appraisal), namely, perceived threat vulnerability (the probability of a threatening event in case of non-compliance), perceived threat severity (the gravity of event consequences in case of non-compliance), and rewards associated with compliance. For the estimation of the individual capability of compliance (i.e., coping appraisal), three variables are used: response efficacy (the effectiveness of reducing or removing the threat to security if s/he complies with the security policy); self-efficacy (individual's capability to perform the required actions needed to comply with the security policy); and response cost (the cost associated with complying with the information security policy, whether this cost is losing money, time, or effort, affects his/her intention to comply).

For example, if an employee feels that their non-compliance with the policy would make the organization highly vulnerable to security attacks (i.e., high perceived threat vulnerability), their intention would likely be more favorable toward complying. Similarly, if an employee perceives that complying with the information security policy would make performing work more difficult (i.e., response cost), and this outweighs the employee's beliefs about the advantages gained from complying, the employee's intention will likely be less favorable toward complying.

3.2.3 Research Model 2

Prior empirical research using PMT variables has reported inconsistent results, which could be explained by the employees' differing perception of the work-life domain as shaped by BYOD contextual factors. Depending on whether they interpret a specific BYOD usage scenario as being part of their work or life domain, employees' security behavior will likely be impacted by different factors.

Ownership of the device(s) used could influence the factors that affect information security-related behavior changes. For instance, the positive effect of perceived threat severity on compliance with information security policy was only supported when employees were using organizational devices (Vance et al., 2012; Pahnila et al., 2013; Siponen et al., 2014; Johnston et al., 2015), and not their own devices (Crossler et al., 2014; Dang and Pittayachawan, 2015). In addition, the significant impact of perceived threat vulnerability on employees' intention to comply with information security policy was not supported when employees were using their personal devices (Crossler et al., 2014; Dang and Pittayachawan, 2015).

This evidence was also shown for the contextual factor of location. Li and Siponen (2011) argued that the variables influencing information security behavior at home are different from those influencing it in the workplace; thus, usage of the device at home differs from usage of the device in the workplace regarding information security-related behavior. For example, an employee in the workplace has a different sense of awareness of factors, such as organizational information security monitoring controls, sanctions, rewards, and reputation, compared to an employee at home or otherwise outside of the workplace. This change in their sense of awareness can affect employees' information security compliance behaviors. Dang-Pham and Pittayachawan (2015) studied the impact of this contextual factor by examining students' information security compliance behaviors when at home and at university. The results indicated that certain factors have different impacts on information security behaviors; for example, perceived threat vulnerability had an impact on students' information security compliance behaviors when they were located at the university but had no impact on their information security compliance behaviors at home.

Notably, the same arguments apply to the type of activities and data sensitivity. Previous information security behavior literature has examined the influencing factors with regard to BYOD work-related activities (Crossler et al., 2014), and personal activities (Dang and Pittayachawan, 2015). In the workplace setting, Crossler et al. (2014) found that perceived

threat vulnerability did not affect employees' intention to comply with information security policy when they performed work-related activities, while Dang-Pham and Pittayachawan (2015) showed that for non-work activities, it did have an impact. In addition, Crossler et al. (2014) investigated the impact of information sensitivity on information security behaviors using the nature of the participants' jobs as a proxy for data sensitivity: they argued that accountants deal with more sensitive information compared to non-accountants. The result of their study showed that perceived threat severity affected policy compliance behavior for accountants, while the effect was insignificant for non-accountants.

Existing research on information security has shown that users are influenced by different factors depending on whether they are in the work or the home environment. Thus, depending on whether they interpret a specific BYOD usage scenario as being part of the work or the life domain, employees' security behavior will likely be impacted by different factors. However, in some BYOD usage scenarios, a blurred border between the life and work domains might cause employees to blend the two, in line with border theory. Despite the limited evidence due to a paucity of studies, it seems that BYOD contextual factors alter the relative importance of other factors in explaining security behavior. This research argues that making sense of BYOD usage scenarios from the work-life domain perspective is one of the underlying reasons for such a difference. For instance, perceived threat vulnerability is more relevant to BYOD usage scenarios that are interpreted as being in the work domain rather than the life domain. This might be due to the perception the employees might have due to the usage of organizational assets and his/her heightened fear of a breach. In such a case, the perceived threat vulnerability factor will shape employees' behavior when they are at work, but not when they are at home. The same argument can be made for perceived threat severity—that it might be relevant in the work but not in the life domain.

Based on the above arguments and on PMT, this research puts forward the following hypotheses:

H6*: The effect of employees' perceived threat severity on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.*

***H7**: The effect of employees' perceived threat vulnerability on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.*

***H8**: The effect of employees' anticipated rewards on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.*

***H9**: The effect of employees' perceived response efficacy on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.*

***H10**: The effect of employees' perceived self-efficacy on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.*

***H11**: The effect of employees' response cost on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.*

Based on the above hypotheses, Figure 6 shows the second research model that was developed to achieve the second aim of this study. The model aims to understand the impact of employees' interpretations of whether they are in the work or life domain on their security-related behavior. This model adopted the same control variables as those used in Model 1.

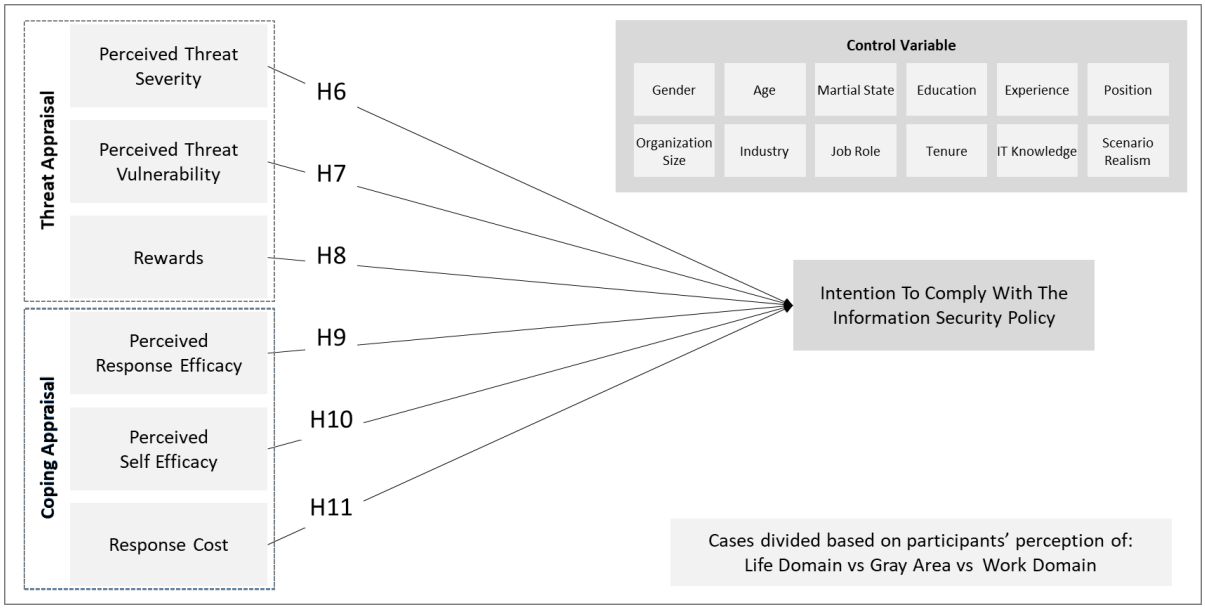


FIGURE 6: RESEARCH MODEL 2

3.3 Chapter Summary

Based on the review of the literature, this chapter proposed the use of BYOD contextual factors based on border theory. There are five contextual factors: 1) device ownership—capturing whether the device is owned by the employee or the organization s/he works with; 2) employee location—capturing whether the employee is on the work premises or not; 3) time of activity—whether it is during working hours or not; 4) type of activity—whether it is work-related or personal; and, 5) sensitivity of the data—whether this data is personally owned or owned by the organization.

Based on bring your own device contextual factors, two research models were presented in order to address the gaps identified in the literature. The first model aims to examine the effect of each contextual factor on employees' perception of the work-life domain. The second model uses protection motivation theory in order to show how employees' perception of whether they are in the life or work domain affects variables influencing their intention (or not) to comply with the information security policy. These two models will provide a conceptual illustration of how, ultimately, bring your own device contextual factors affect employees' intention to comply with information security policies.

The next chapter discusses the research methodology and presents how these models will be tested.

CHAPTER FOUR: RESEARCH METHODOLOGY

To address the research question, the previous chapter discussed the two research models proposed in this study and presented the hypotheses associated with the two models. This chapter presents the research methodology, including the philosophical assumptions, sample, procedure, instruments, and statistical techniques used to test the research hypotheses.

4.1 Philosophical Assumptions

Depending on the philosophical assumption adopted, positivist, interpretive and critical are three possible paradigms for conducting research (Crotty, 1998; Scotland, 2012). The positivist paradigm assumes objectivity of reality, which can be measured independently from the researcher, and this paradigm aims to improve the predictive understanding of phenomena by testing theories (Crotty, 1998; Scotland, 2012; Cohen et al., 2013). The interpretive paradigm assumes the subjectivity of reality, which differs for each individual, and this paradigm aims to uses the meaning individuals assign to the phenomena in order to better understand it (Crotty, 1998; Scotland, 2012; Cohen et al., 2013). The critical paradigm assumes that history shapes reality, which is constructed socially, and this paradigm aims to seek human emancipation by examining the conflicts in contemporary society (Crotty, 1998; Scotland, 2012). Each of these paradigms has its own advantages and disadvantages and affects how research is conducted and the principles it should adhere to (Crotty, 1998; Scotland, 2012; Kumar, 2019).

Based on the research question and objectives of this study, the underlying philosophical assumption for this study is classified as a positivist paradigm. The positivist paradigm's ontological position, as stated above, is that of realism which has the view that objects exist independently from the researchers (Crotty, 1998). Thus epistemologically, positivist studies aim to research certain and demonstrable knowledge about an objective reality that is not influenced by the researcher's conscience (Crotty, 1998). In positivist studies, the phenomena are researched to provide causal inferences for the relationship between the independent variable and one or more dependent variables based on empirical tests (Cohen et al., 2013). Looking at the research question and objectives of this study, they fall into the positivist paradigm as they showed a relationship between multiple variables that can be empirically tested, and the answer to this research question has the potential to add to the existing body of knowledge.

Due to the nature of the positivist paradigm that aims to provide predictions and generalize the results, usually the methods used will generate quantitative data (Scotland, 2012). Accordingly, quantitative methods are one of the main methods used in positivist studies (Crotty, 1998; Kumar, 2019). Quantitative methods are of an objective nature that is best used if the sample size is big, and if the study is seeking generalization of the result (Myers, 2009). Thus, this study will adopt a quantitative approach to design the research and test the hypotheses.

The method, regardless of which is selected, will shape the whole aspect of the study design (Kumar, 2019). The next section will provide details on the research design and the quantitative methods used to conduct the study.

4.2 Research Design

To test the proposed research models, four steps were followed (see Figure 7). First, a base hypothetical scenario was developed to aid the employees when responding to the survey and to encourage them to avoid concealing their true intentions (e.g., Higgins et al., 2005; D'Arcy et al., 2009; Hu et al., 2011). Then, the scenario was developed to capture the BYOD contextual factors and to determine the impact of the employees' interpretations of the work-life domain. Third, a survey was developed as the primary tool for obtaining the required data to test the two models proposed in this study. According to Fishbein and Ajzen (2010), a self-reporting mechanism is ideal for investigating general behaviors. In addition, a survey is a common method for collecting data to study information security behaviors (e.g., Herath and Rao, 2009b; Bulgurcu et al., 2010a; Ifinedo, 2012), and a survey panel was used for the data collection. Finally, a regression analysis was used to analyze the collected data.

The following sections describe the behavior of interest (complying with the information security policy), scenario development, measurement development, and the sampling and data collection.

FIGURE 7: RESEARCH DESIGN

4.2.1 Scenario Development

Because this research relies on self-reporting as the primary method for data collection, certain limitations are expected; for example, an employee might not reveal their true intentions about complying with the information security policy in their organization. Bulgurcu et al. (2010a) suggested using scenarios to minimize the impact of this limitation. Using scenarios is a technique that "present[s] subjects with written descriptions of realistic situations and then request[s] responses on a number of rating scales that measure the dependent variables of interest" (Trevino, 1992, pp.127–128, cited in Myyry et al., 2009). Therefore, many studies use scenarios to overcome such limitations (e.g., Higgins et al., 2005; D'Arcy et al., 2009; Hu et al., 2011).

In addition, scenarios provide the required tool to answer the research question and achieve the objectives of this research because they allow the creation of a realistic situation where some factors can be manipulated and tested more effectively. In this research, the scenarios provide a realistic situation that reflects the BYOD contextual factors and the different usage scenarios they create. The aim is to categorize the respondents into one of three groups based on their perceptions of the work-life domain resulting from the BYOD contextual factors. The first group (i.e., the life domain group) will mostly interpret the scenario as a life domain; the second (i.e., the work domain group) will interpret the scenario as a work domain; and the third (i.e., the gray area group) will tend to capture a grayer interpretation of BYOD usage scenario by blurring the boundaries between the life and work domains.

To develop the required scenarios, first, a common and important behavior relevant to the domain of the study needs to be selected. A review of the different behaviors related to the study was, therefore, conducted to shortlist the most important and common behaviors to use in the scenarios. In previous studies, some authors have used open-ended web-based questionnaires to elicit the specific behaviors of interest (Siponen and Vance, 2010; Vance and Siponen, 2012; Vance et al., 2012), while others have conducted a review of the literature to define the behavior of interest (Guo et al., 2011; Guo and Yuan, 2012; D'Arcy et al., 2014). Based on an extensive review of the literature, this research adopted the latter approach where behaviors used in previous studies' scenarios were reviewed and selected to be part of this thesis' scenario development.

Table 4 lists the 13 key behaviors identified in the literature review. The most used behavior was 'USB Drive Usage,' which was used in seven articles, followed by 'Password Sharing'

and ‘Unauthorized Access,’ which were used in six articles. ‘Logging Off’ was the next most used behavior, which was identified in five articles. ‘Writing Down Passwords’ and Unauthorized Software Installation’ were both used in three articles. ‘Public Network Usage’ and ‘Unauthorized Modification’ were employed in two articles, and ‘Password Change,’ ‘Failure to Report Security Incident,’ ‘Usage of Device by Unauthorized Users,’ ‘Performing Non-Work Related Activities,’ and ‘Unauthorized Disclosure’ were each used once.

TABLE 4: IDENTIFIED BEHAVIORS USED IN PREVIOUS SCENARIOS IN THE LITERATURE REVIEW

Behavior	Number of Articles	Articles
USB Drive Usage	7	Siponen and Vance (2010); Guo et al. (2011); Guo and Yuan (2012); Vance and Siponen (2012); Vance et al. (2012); D'Arcy et al. (2014); Johnston et al. (2015)
Password Sharing	6	Myyry et al. (2009); Siponen and Vance (2010); Vance and Siponen (2012); Vance et al. (2012); Barlow et al. (2013); D'Arcy et al. (2014)
Unauthorized Access	6	D'Arcy and Hovav (2007); D'Arcy and Hovav (2009); D'Arcy et al. (2009); Vance et al. (2012); Cheng et al. (2013); Johnston et al. (2016)
Logging Off	5	Siponen and Vance (2010); Vance and Siponen (2012); Vance et al. (2012); D'Arcy et al. (2014); Johnston et al. (2015)
Writing Down Passwords	3	Guo et al. (2011); Guo and Yuan (2012); D'Arcy et al. (2014)
Unauthorized Software Installation	3	D'Arcy et al. (2009); Guo et al. (2011); Guo and Yuan (2012)
Public Network Usage	2	Guo et al. (2011); Guo and Yuan (2012)
Unauthorized Modification	2	D'Arcy and Hovav (2009); D'Arcy et al. (2009)
Password Change	1	Johnston et al. (2015)
Failure to Report Security Incident	1	Vance et al. (2012)
Usage of Device by Unauthorized Users	1	Vance et al. (2012)
Performing Non-Work Related Activities	1	D'Arcy et al. (2009)
Unauthorized Disclosure	1	D'Arcy et al. (2014)

Based on the results of the literature review, and in support of the objectives of this research, the most relevant behavior was considered to be “logging off”. Some of the behaviors were excluded due to their inability to accommodate all the defined BYOD contextual factors. For example, ‘password sharing’ behavior, although used relatively frequently in the information security literature, was not considered an optimal behavior for this study because one of the contextual factors is conducting work-related and personal activities and it was assumed that employees would not see organizational information security policies as applying to their personal data. A similar situation arises with ‘Unauthorized Access’ behavior because it is unlikely that this behavior is applicable to personal activities. Although ‘USB Drive Usage’ is applicable to all BYOD contextual factors, its relevance might not apply to all organizations that do not apply this usage to employees’ personal devices; if this usage can be blocked by default, or if the employee does not have the freedom to choose whether to comply or not with the information security policy then it will not provide the right scenario to test these research hypotheses. ‘Logging off’ behavior was thus selected as the behavior for the scenario development because it applies to all BYOD contextual factors and is used frequently in the information security literature.

After defining the behavior to be used in the scenarios, the scenarios need to be developed to ensure that they contain the required context for the study objectives in terms of the behavior and manipulation to be examined. The scenarios can provide the required context, state a certain behavior that has been performed, and/or provide a mechanism for manipulating the BYOD contextual factors. While Myyry et al. (2009) used scenarios only to provide a context, other researchers stated that the actor in the scenario has to perform a certain behavior to overcome the challenge of employees’ tendency to conceal their true information security-related intentions (D'Arcy et al., 2009; Siponen and Vance, 2010; Vance and Siponen, 2012; D'Arcy et al., 2014). Further, other studies have used scenarios to manipulate factors related to the behavior of interest (D'Arcy et al., 2009; Chen, 2012; Barlow et al., 2013). Accordingly, as shown in Table 5, the scenario for this study was developed based on scenarios used in prior literature (Vance and Siponen, 2012; Barlow et al., 2013; D'Arcy et al., 2014; Johnston et al., 2015) and includes a base scenario to provide a context in which the behaviors of interest for this research can be performed and tested. In addition, the scenario includes a non-compliant information security behavior that was performed by an actor to facilitate capturing the true intention of the respondents. Further, the manipulation statements related to the BYOD contextual factors and their placeholder in the base scenario are defined.

TABLE 5: BASE SCENARIO AND BYOD CONTEXTUAL FACTORS STATEMENTS

XYZ company have recently adopted a bring your own device policy. The company provides its employees with the option of providing them with a company-owned laptop or the employees can choose to bring their own laptop. If an employee opted to bring his/her laptop, then the laptop will be granted access to the company's information systems in order for the employees to be able to perform their day-to-day tasks and will be subjected to company's information security policy.

John is an employee at XYZ company. [Insert Device statement here]. Due to the nature of his job, John is aware that his laptop contains [Insert Sensitivity statement here]. [Insert Data statement here]. One day at [Insert Place statement here] [Insert Time statement here], John logs into the laptop to [Insert Activity statement here]. "After some time, John is in need of a restroom break. He is aware of the company's policy that requires users to log off their laptop when not in use. However, John hates the inconvenience of logging out and logging back in again, so he does not log off his laptop when he leaves to visit the restroom." (D'Arcy et al., 2014 p.313)

Device ownership	Owned By Employee:	Owned By Organization:
	He is one of the employees who choose to bring their own laptop and integrate it with the company's information systems	He is one of the employees who choose to use a company-owned laptop.
Employee's Location	Home:	Work:
	Home	Work
Time of Activity	Non-Working Hours:	Working Hours:
	After working hours	During working hours
Activity Type	Personal:	Work Related:
	Book his vacation	Complete a task requested by his direct manager
Data Sensitivity -Company Data	Low Sensitivity	High Sensitivity
	Only non-sensitive company data	Sensitive company data
Data Sensitivity -Personal Data	Personal Data (sensitive):	Personal Data (non-sensitive):
	In addition, John has sensitive personal data stored on the laptop	In addition, John has non-sensitive personal data stored on the laptop

To ensure that the contents are clear, relevant, and realistic and that they provide the required manipulation of BYOD contextual factors to test the research hypothesis, both information security experts and academic professionals were asked to review the developed scenarios. The scenarios were updated based on their feedback. This expert review aligns with prior research in which reviews of the developed scenario with panels or security experts and academics were

conducted to ensure their realism and manipulation effect (Vance and Siponen, 2012; Vance et al., 2012; Barlow et al., 2013).

Further, the survey included a set of items to check that respondents found the scenarios realistic and to confirm the accuracy of the manipulation. Some prior studies have used items to check the scenarios' realism (e.g., Siponen and Vance, 2010; Barlow et al., 2013; Johnston et al., 2016) and in this study, four items were used to measure the scenario's realism (i.e., the situation described in the scenario could occur in real life). In addition, others have deployed items in order to ensure that the manipulation of factors has been effective on the participations when reading the scenarios (Johnston et al., 2016). In this study, six items were used to ensure the effectiveness of the scenarios' manipulation, one for each contextual factor (i.e., device ownership, sensitivity for company data, sensitivity for personal data, place, activity, and time). Based on the existing literature, items were adopted and included in the final survey, as shown in the next section and presented in Appendix C, Measurement Items.

After defining the behavior to be used in the scenarios, a decision was made about how many scenarios to present to each respondent. Prior research has used multiple methods, such as using one scenario for all respondents, presenting each respondent with one of a random set of scenarios, or showing each respondent several scenarios. Myyry et al. (2009) used one scenario for all respondents and reported this as a limitation. Other researchers presented each respondent with more than one scenario (e.g., Chen, 2012; Barlow et al., 2013; Johnston et al., 2016); however, this can cause response fatigue because it requires each respondent to take more than one survey. To overcome the challenges of these two approaches, many studies developed more than one scenario but presented only one randomly selected scenario to each respondent (e.g., Siponen and Vance, 2010; Guo et al., 2011; Guo and Yuan, 2012; Vance and Siponen, 2012; Vance et al., 2012; D'Arcy et al., 2014; Johnston et al., 2015). Similar to this stream of research, this study presented each respondent with one scenario selected randomly from a pool of scenarios that were built from a combination of the base scenario and the manipulation statements related to the BYOD contextual factors.

4.2.2 Measurements Development

As stated at the beginning of this chapter, this study used a survey method for the data collection; this aligns with existing literature in this domain that mostly used surveys to study information security behaviors (e.g., Herath and Rao, 2009a; Bulgurcu et al., 2010a; Ifinedo, 2012). Further, it is recommended to use already tested and validated survey questions to

improve the reliability of the results (Straub, 1989; Boudreau et al., 2001; Straub et al., 2004). Accordingly, an extensive literature review was conducted to identify items that could be used to test the two proposed research models. Only measurements with high validity and reliability were selected from the literature; a total of 50 items (see Appendix C) were used to measure the two proposed research models. Hair et al. (2010) recommend a minimum of three items per variable, although four items are preferable. These items are measured on a seven-point scale as recommended in the literature (Fishbein and Ajzen, 2010). The study adheres to this recommendation, whenever possible, to measure the constructs in the proposed models.

For the first model, the perception of work-life balance was used as the dependent variable and was measured using two items. The items asked the respondents to evaluate whether they believed the scenario presented was in the life domain or in the work domain. Their evaluation was captured by presenting the following two items to the respondents: "If I were using the laptop in the same scenario, then I would believe that I am in my work/life [choose one] domain" and "In the scenario presented, John's usage of the laptop feels more like he is in his work/life [choose one] domain".

To measure the BYOD contextual factors, one item was used for each, and the respondents were asked to define the BYOD contextual factor presented in the scenario. For device ownership, respondents were asked whether the actor in the scenario used his own device or a company-provided device. For data sensitivity, the respondents were asked to describe whether the action involved sensitive or non-sensitive and whether it was company or personal data. They were also requested to define the type of activity performed by the actor in the scenario as either personal or work-related and to identify the location the activity was performed in – at home or at work. Finally, for the time factor, respondents were asked to state whether the activity in the scenario was performed during working or non-working hours.

For the second model, to measure the employees' intentions to comply with the information security policy (i.e., the dependent variable for the second model), three items were used (Ifinedo, 2012). The participants were asked to evaluate their intention to comply with the information security policy by responding to sentences such as, "It is possible that I will comply with the requirements of my organization's information security policy to protect the organization's information systems."

To measure the PMT variables, 24 items were selected. Each PMT variable was measured using four items. Perceived threat severity was measured using items such as, “I believe that protecting my organization’s information is . . .” (Ifinedo, 2012 p.92). Perceived threat vulnerability was measured by asking participants to respond to statements such as, “I know my organization could be vulnerable to security breaches if I don’t adhere to the requirements of my organization’s information security policy” (Ifinedo, 2012 p.92). The reward component comprised items such as, “My pay raises and/or promotions depend on whether I comply with the requirements of my organization’s information security policy” (Bulgurcu et al., 2010a p.537). With regard to response efficacy, participants were asked to evaluate their perception of the effectiveness of security measures and their compliance with the information security policy by responding to statements such as, “Every employee can make a difference when it comes to helping to secure the organization’s information security” (Workman et al., 2008 p.2808; Herath and Rao, 2009b p.122; Ifinedo, 2012 p.92). Response cost was measured by asking participants to evaluate the cost associated with the security measures and their compliance with the information security policy by responding to statements such as, “The impact on my work from recommended security measures is . . .” (Workman et al., 2008 p.2809; Ifinedo, 2012 p.92). Finally, for perceived behavioral control, four items were used, including measurements for both the capacity (e.g., judgment of how easy or how difficult is it for the employee to comply) and the autonomy (e.g., judgment of whether compliance is within the control of the individual) aspects of perceived behavioral control (Fishbein and Ajzen, 2010). Participants were also asked to evaluate themselves by responding to statements such as, “For me to comply with the requirements of my organization’s information security policy would be . . .” (i.e., capacity aspect of perceived behavioral control) and “The number of external influences that may prevent me from complying with the requirements of my organization’s information security policy are . . .” (i.e., autonomy aspect of perceived behavioral control) (Sheeran and Orbell, 1999 p.356; Al-Omari et al., 2013 p.3027).

In addition to the measures selected for the main constructs in the two proposed models, participants were asked to respond to demographic questions relating to gender (Park and Jex, 2011; Berkowsky, 2013; Xie et al., 2018), age (Berkowsky, 2013; Xie et al., 2018), marital status (Park and Jex, 2011; Berkowsky, 2013; Xie et al., 2018), education (Berkowsky, 2013), experience (Johnston et al., 2015), position (Berkowsky, 2013), organization size (Bulgurcu et al., 2010a), industry (Bulgurcu et al., 2010a), job role (Herath and Rao, 2009b), tenure (Son,

2011), and IT knowledge (Bulgurcu et al., 2010a). These data were required to classify the responses and to consider their effects when testing the models.

Prior to starting the data collection process, two academics and two practitioners reviewed the measurements to ensure that the items were relevant and to confirm their face validity. Hair et al. (2010, p.710) stated that "face validity is the most important validity test" and similar information security studies have also performed this step to review the measurements and ensure the content validity of the items contained in the survey (e.g., Lee and Larsen, 2009; Vance et al., 2012). Based on the review, the items were modified and updated.

After concluding the review process, a pre-test was conducted. Because the items used in this research are borrowed from different studies, it is recommended to test them with a population close to the targeted population prior to conducting the data collection process (Hair et al., 2010). The pre-test also helps to purify the measurements (Hair et al., 2010). Such practices have also been used in the information security literature (e.g., Vance et al., 2012; Vance et al., 2013). A sample of 50 was used for the pre-test. After completing the pre-test and confirming the adequacy of the measurement model, the study proceeded with the data collection process.

4.2.3 Data Collection

Existing information security literature has often used web-based surveys to collect data (e.g., Zhang et al., 2009a; Bulgurcu et al., 2010a; Yoon and Kim, 2013; D'Arcy et al., 2014). This thesis also did so, the survey questionnaires being prepared and then uploaded to the web-based survey tool, Qualtrics.

To improve the response rate and reduce the refusal rate, Malhotra (2010) suggests notifying the participants about the objectives of the research prior to them starting the survey. Accordingly, the final questionnaire included a participant information sheet presenting the purpose of the research, the researcher's name and contact details, the requirements of the participants, and possible risks and discomforts. The information sheet also provided an ethical review, complaint process and requested their consent to participate. A motivational message was also included in the participant information sheet to inform the respondents of their importance to the success of the research and to explain how the research will contribute to society in terms of helping to improve organizational data security.

The survey was designed to reduce measurement error by paying attention to the survey layout, format, and order (Ng et al., 2009). In addition, each question was identified with a numeric label, and the questions were organized into sections to minimize confusion.

Each participant was randomly presented with one scenario based on the BYOD contextual factors, which was generated by the survey tool, Qualtrics. After reading their scenario, all participants were presented with the same set of questions, divided into two main sections. The first section comprised items that capture the concepts for the two models in this research. The second section obtained demographic and control items. After completing the survey, the participants were presented with a thank you note.

An online panel service was used to recruit the participants for the data collection. Behrend et al. (2011) state that an online panel provides a better representation of the target sample for research that targets employees, rather than university-based samples, as it can obtain older, more diverse, and more experienced respondents. Further, they stated that samples from panels could provide reliable data that can be better than university-based samples, and they showed that, from a social desirability viewpoint, panels provide better results than those obtained from university sample-based research. Their study provided evidence that the data captured through the panel study is of at least as good quality as that captured by other social science research that uses undergraduate students to represent the employee segment. Other studies have reported similar results, showing that online panels are a reliable tool for data collection (e.g., Paolacci et al., 2010; Alonso and Baeza-Yates, 2011; Barger et al., 2011; Buhrmester et al., 2011).

The usage of online panels to recruit participants is evident in several information security studies. D'Arcy, Herath, and Shoss (2014) used a market research firm to recruit participants for their data collection; they stated that panels are far advantageous over other methods with regard to ensuring anonymity, thus increasing the probability of obtaining more honest responses, especially to questions that may prompt participants to respond with what they think are more socially desirable answers. Further, they stated that panels are able to provide a sample from various organizations with diverse demographics that would be difficult to get from other methods, thus reducing the potential bias that may occur from unique organizational factors. Similarly, Posey, Bennett, and Roberts (2011) stated that for topics as sensitive as information security, it is difficult to obtain accurate responses, and many organizations may also prevent external parties from studying this topic. They therefore utilized an online panel provider to

recruit their participants who were guaranteed anonymity in order to provide better quality data. Burns et al. (2017) also used online market research to collect data due to its ability to provide increased anonymity; respondents are aware/reassured that their privacy is protected and they can complete the survey outside of their work environment. These conditions provided by anonymity and the off-site access to self-reporting surveys are recommended by methodologists to eliminate common methods bias and have been adopted by many studies of a sensitive nature (Burns et al., 2017). Further, Burns et al. (2017) stated that panels increase representation of the sample of the targeted population. Bulgurcu et al. (2010a) adopted a similar approach by using a professional market research company to obtain their sample. Barlow et al. (2013) also recruited participants through a market research firm which identified qualified survey respondents. Other information security studies have also used such services for the data collection process (e.g., Posey et al., 2015; Johnston et al., 2016; Tsai et al., 2016; Yazdanmehr and Wang, 2016; Han et al., 2017; Menard et al., 2017; Sharma and Warkentin, 2018). Following the same approach, this research used the online panel provider, Prolific (https://www.prolific.co), to recruit the desired sample.

This study also offered a monetary incentive to participants. Malhotra (2010) suggested providing incentives to the participants to increase the participation rate, provided that the actual amount offered does not enhance the response bias. This approach has been adopted effectively in previous behavioral studies (e.g., Brubaker and Fowler, 1990; Sanderson and Jemmott, 1996). Providing incentives to participants to increase the response rate is common in information security behavioral studies irrespective of whether participants were recruited via online panel provider or directly (e.g., Boss et al., 2009; Herath and Rao, 2009a; Herath and Rao, 2009b; Ng et al., 2009; Posey et al., 2011; Guo and Yuan, 2012; Barlow et al., 2013; Cheng et al., 2013; D'Arcy et al., 2014; Shropshire et al., 2015). This study offered a minor monetary incentive, where each participant was paid £0.85 for successfully completing the survey. This aligned with prior studies in information security behavioral and other behavioral studies.

To increase the data quality, eligibility criteria were applied. The first eligibility criterion was based on the approval rate of potential participants' previously submitted responses to other studies. In order to increase the quality of data gathered by reducing the chance of receiving responses from participants who are disengaged or who give random answers, only participants with an approval rate equal to or higher than 90% could participate in this research. In addition,

using an online pool of participants allowed us to target specific groups of participants. This research targeted employed individuals to capture their perceptions of and beliefs about information security compliance in relation to BYOD. Accordingly, the eligibility criteria included employed status as another criterion for participation in the survey. Based on these two eligibility criteria, prolific identified a total of 12,962 eligible participants out of its 68,772 participant pool during the one month period in 2017 that the survey ran.

Further, the usage of incentives, the eligibility criteria, and the assurance of participants' anonymity reduced any effect of non-response bias. Additionally, as stated above, the use of online panels for data collection enhances the quality of collected data and better reaches the desired sample.

From the 12,962 eligible participants, 3,035 responses were collected. All the questionnaire items were completed. As presented in Table 6, the descriptive analysis shows that there were more female respondents (59.1%) than male (40.9%). Most of the participants were middle-aged individuals (40.5%), with 72.2% aged 25–44, 6.5% aged younger than 25, and 21.4% older than 44. Just over half were married (50.3%), while just under 40% had never been married (39.9%). More than half of the respondents had a bachelor's or higher degree (66.6%), and the remainder either had a high school degree or had not finished high school. Around half of the respondents had over 10 years of work experience (51.9%), 22.45% between 5 and 10 years, 15.9% 2 to 5 years, and the remaining 9.8% less than 2 years' work experience. Almost 60% of the respondents were mid-level personnel (58.45%), almost one-third identified themselves as junior staff (27.7%) and the remainder were top management personnel (13.95%). In terms of organization size, 35.2% of the respondents worked in organizations with fewer than 100 staff members, 18.6% in organizations with 100–499 staff, 10.5% in organizations with 500–999 staff, 13.3% in organizations with 1,000–4,999 staff and the remaining 22.5% in organizations with more than 5,000 staff. Most of the respondents held non-IT positions (76.8%), and the remainder worked in the IT field (23.2%).

TABLE 6: DEMOGRAPHICS AND CHARACTERISTICS OF THE SAMPLE (N = 3,035)

Variable	Category	Percentage
Gender	Male	40.9
	Female	59.1
Age	18–24	6.5
	25–34	40.5
	35–44	31.7
	45–54	15.3
	55–64	5.6
	65–74	0.4
	75–84	0.1
Marital Status	Married	50.3
	Widowed	0.9
	Divorced	6.7
	Separated	2.2
	Never married	39.9
Religion	Christian	47
	Jewish	1
	Muslim	2.4
	Buddhist	2.2
	Hindu	0.8
	Atheist	30.3
	Other	16.4
Nationality	South America	1
	North America	24.6
	Europe	70
	Asia	3.3
	Africa	0.2
	Australia	0.8
Education	Lower than high school	1.3
	High school graduate	32.2
	University or bachelor's degree	45.5
	Master's degree	16.9
	Doctorate degree	4.2
Experience	Less than 6 months	1.5
	6–12 months	3
	1–2 years	5.3
	2–5 years	15.9
	5–10 years	22.4
	More than 10 years	51.9

Variable	Category	Percentage
Rank	Top management personnel	13.9
	Mid-level personnel	58.4
	Junior staff	27.7
Organization Size	Fewer than 100	35.2
	100–499	18.6
	500–999	10.5
	1,000–4,999	13.3
	5,000–10,000	8.3
	More than 10,000	14.2
Industry	Education	13.9
	Financial services	8.1
	Government	7.6
	Food/beverage	3.5
	Healthcare	10.5
	Manufacturing	8
	Non-profit	4.9
	Medical, biotechnology, pharmacology	1.9
	Real estate	1.9
	Services	14.2
	Information technology	12
	Telecommunications	2.7
	Travel	1.9
	Wholesale/retail	8.7
Role	IT	23.2
	Non-IT	76.8
Tenure	Less than 3 months	4.2
	3–6 months	5.4
	6–12 months	9.4
	12–60 months	35.4
	More than 60 months	45.7
IT Knowledge	Very Low	0.8
	Low	2.7
	Somewhat Low	6.8
	Medium	15
	High	33.4
	Somewhat High	23.8
	Very High	17.6

Almost half of the respondents had worked in their current organizations for more than five years (45.7%), one-third for one to five years (35.4%), and the remainder for less than one year (19%). In addition, the respondents came from different industries, with the majority working in the service industry (14.2%); the industries with the fewest participants were medical, real estate, and travel (1.9% each). The majority identified themselves as having high to very high knowledge of IT (81%), the others claiming medium to low knowledge of IT (19%). Table 6 summarizes the participants' demographics and characteristics. Based on the demographics, the sample was considered a fairly representative target because it included employees of different ages, genders, and marital statuses, with different education levels (e.g., high school, bachelor, PhD), different job levels (e.g., manager, mid-level, entry), and different years of experience, tenure, and roles (e.g., IT, non IT), and from different organizations and industries.

4.2.4 Data Analysis

Multiple regression analysis is a multivariate technique that makes it possible to examine the relationship between multiple independent variables with a single dependent variable (Hair et al., 2010). Many prior studies of employee compliance with information security policy have adopted this technique (e.g., Harrington, 1996; Skinner and Fream, 1997; Siponen et al., 2007; D'Arcy and Hovav, 2009; Myyry et al., 2009; Ng et al., 2009; Posey et al., 2011; Sommestad et al., 2015). Therefore, in order to test the two models used in this study, the data were analyzed using multiple regression analysis.

4.3 Ethical Consideration

All participants were provided with a participant information sheet that provided the required information about the study. Their privacy was assured as all the information collected was anonymous and could not be tracked to any individual participant. Further, consent was requested from the participants in order to use the provided data. All ethical guidelines provided by the University of Wollongong in Dubai were followed, and ethical approval was gained from the university.

The participants were presented with an information sheet which defined the research's purpose, and stated the researcher's name and contact details, the expected requirements of the participants, and possible risks and discomforts. It also included the details of the ethical review process and the complaint process. Finally, consent was requested from all participants.

Since data were collected anonymously, confidentiality was maintained thoughout the research. All research data were only accessible by the researchers and none of these data can be traced back to the participants. Any access to these data from any party will only be provided after getting approval from the ethics department at the University of Wollongong in Dubai.

4.4 Chapter Summary

The chapter discussed which research methodology was suitable for the study and the choice of quantitative methods from a positivist paradigm perspective was explained. Similar to many other studies focused on information security behaviors, a base scenario was developed to be presented to the participants that would 1) provide the context via a hypothetical situation, 2) manipulate the BYOD contextual factors, and 3) reduce social desirability bias. In addition to the scenario, an online survey was developed based on previously tested items from other information security studies in order to capture all the data related to the two models of this study. In addition, the survey was reviewed by two information security professionals and two academics to ensure face validity and clarity for the participants. The data was collected using an online platform service in order to provide better anonymity and higher quality data as recommended in many other studies. Each participant was supplied with a participant information sheet that contained all of the required information about the study, contact details for the researcher and the ethical committee in UOWD, assured their anonymity and asked them to provide consent. Once the participants had read the participant information sheet and agreed to participate, they were presented with a random automated generated scenario based on the designed manipulation from BYOD contextual factors. After reading the scenario, participants were provided with the survey and, upon successfully completion of the survey, paid a monetary incentive. The data collected from this procedure will be analyzed using multiple regression analysis in the next chapter.

CHAPTER FIVE: DATA ANALYSIS AND RESULTS

The previous chapter presented the research design, describing the process of scenario development, the output of this process, the instrument used to conduct the survey, and the method of data collection. This chapter will provide a detailed data analysis and describe the results of this analysis. It will start by describing the technique that was used to analyze the data. Then it will detail how the data were prepared for analysis. Finally, the models in this study will be tested, and the results will be presented.

5.1 Data Preparation

To prepare the data, it was first exported from the Qualtrics website; 3305 responses were included. The data were then imported into SPSS, where each piece of data was coded with an acronym to simplify interactions with the data. Before analysis, the data were prepared for multiple regression analysis. Therefore, the data were examined to address issues of missing data, to ensure adherence to multiple regression analysis assumptions, and to confirm the validity and reliability of the instruments.

5.1.1 Missing Data

From the data imported into SPSS from Qualtrics, 270 responses were deleted because they were found to be incomplete, resulting in a total of 3035 usable responses. A test for missing data was conducted to check for unengaged observations. As stated by Hair et al. (2010), an observation that is missing less than 10% of the data can be ignored. The test for missing data showed that no responses contained more than 10% missing fields. All of the missing values were in the control variables.

To address the 21 cases that were missing data for 11 variables, missing data were imputed. Hair et al. (2010) recommend the use of imputation methods when less than 10% of the data are missing. A mean substitution method was used to replace the missing values as recommended when relatively low amounts of data are missing (Hair et al., 2010). Using the mean substitution method, the missing values were replaced with the series mean in SPSS for all 21 cases.

5.1.2 Item Reliability

As this study uses multiple items to measure the constructs, it was critical to ensure the reliability of these items before testing the two models used in this study. Cronbach’s alpha

was used to measure their reliability. Based on Hair et al. (2010), a Cronbach's alpha value higher than .70 was considered acceptable. Other studies have also adopted the same thresholds (e.g., Ng et al., 2009; Posey et al., 2011; Alshare et al., 2018)

The reliability test for the four items used to measure Scenario Realism (SR) yielded a Cronbach's alpha of .902, which is higher than .70 and therefore exceeded the lower limit of acceptability (Hair et al., 2010). Similarly, the four items for Perceived Work-Life Domain (PLWD) resulted in a Cronbach's alpha of .756, which is also acceptable. The Cronbach's alpha for items used to measure Perceived Self-Efficacy (SE) was also acceptable: .761. In addition, the four items measuring Perceived Threat Severity (PTS) resulted in an acceptable Cronbach's alpha of .864. The four Perceived Threat Vulnerability (PTV) items also had an acceptable Cronbach's alpha of .876. Reward (RWD) was also measured with four items and had an acceptable Cronbach's alpha of .897. Likewise, the four items for Response Efficacy (RE) had an acceptable Cronbach's alpha of .830. Intention (INTR) was measured with three items and yielded a Cronbach's alpha of .928, which is also higher than the acceptable limit. However, for Reliability Response Cost (RC), the Cronbach's alpha was .642, which is not satisfactory. One item was dropped, resulting in a Cronbach's alpha of .796, indicating acceptable reliability for the remaining three items. The results of the reliability test are shown in Table 7; these items were included in the next step.

TABLE 7: RELIABILITY STATISTICS

Construct	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of Items
Scenario Realism (SR)	.893	.902	4
Perceived Work-life Domain (PLWD)	.756	.756	4
Perceived Self-Efficacy (SE)	.750	.761	4
Perceived Threat Severity (PTS)	.866	.864	4
Perceived Threat Vulnerability (PTV)	.875	.876	4
Reward (RWD)	.894	.897	4
Response Efficacy (RE)	.829	.830	4
Response Cost (RC)	.797	.796	3
Intention (INTR)	.928	.928	3

5.1.3 Exploratory Factor Analysis

Next, the validity of the measurements was confirmed through an Exploratory Factor Analysis (EFA). The results of the EFA indicate the level of confidence in the validity of measurements used (Hair et al., 2010). An EFA has been used in previous studies prior to conducting a regression analysis test (e.g., Posey et al., 2011). Therefore, an EFA test was conducted in the present study.

All of the items that passed the reliability check were included in the EFA (Principal Component) in SPSS. First, the Bartlett test of sphericity was used to determine the appropriateness of factor analysis (Hair et al., 2010). The test was statistically significant (i.e., .000), which indicates that there are sufficient correlations among the variables. This was also supported by the result of the measure of sampling adequacy (MSA); the result of this test was .882, which exceeds the acceptable threshold of .50 (Hair et al., 2010).

Next, Hair et al. (2010) recommend that the communalities be examined to assess whether the items are at an acceptable level. They recommend a threshold of .50, which indicates that half of the variance of each variable was taken into account; if the communality is less than .50, the items do not have sufficient explanation. All items passed this threshold except the fourth item used to measure Perceived Work-Life Domain (PLWD4R = .465) and the fourth item used to measure Perceived Behavioral Control (SE4 = .466). Hair et al. (2010) suggest that such items may be considered for deletion; however, they may also be retained when there is theoretical support, and the items have demonstrated their reliability and validity through use in prior studies. Therefore, the pattern matrix was examined next.

According to Hair et al. (2010), most researchers use a factor pattern matrix to validate the contribution of each item to the construct. The pattern matrix presented in Table 8 includes eight factors instead of nine; Perceived Threat Severity (PTS) and Perceived Threat Vulnerability (PTV) load on the same factors. Since these factors are theoretically different, and the items have been used and tested in prior studies, two EFAs were conducted. The first excluded these two factors, and the second was conducted on only these two factors.

TABLE 8: PATTERN MATRIX – ALL VARIABLES

	Component							
	1	2	3	4	5	6	7	8
PTS3, Perceived Threat Severity	.990							
PTS4, Perceived Threat Severity	.953							
PTS2, Perceived Threat Severity	.922			-.303				
PTV1, Perceived Threat Vulnerability	.646							
PTV2, Perceived Threat Vulnerability	.610			.341				
PTV4, Perceived Threat Vulnerability	.568			.372				
PTS1, Perceived Threat Severity	.514							
PTV3, Perceived Threat Vulnerability	.481			.427				
RWD4, Reward		.944						
RWD3, Reward		.943						
RWD2, Reward		.879						
RWD1, Reward		.756						
SR2, Scenario Realism			.914					
SR1, Scenario Realism			.893					
SR4, Scenario Realism			.865					
SR3, Scenario Realism			.837					
RE1, Response Efficacy				.916				
RE2, Response Efficacy				.877				
RE4, Response Efficacy				.606				
RE3, Response Efficacy				.554				
INT5R, Intention					.971			
INT4R, Intention					.943			
INT6R, Intention					.919			
SE3, Perceived Behavioral Control						.762		
SE1, Perceived Behavioral Control						.758		
SE2, Perceived Behavioral Control						.702		
SE4, Perceived Behavioral Control						.642		
PLWD2, Perceived Work-Life Domain							.860	
PLWD3R, Perceived Work-Life Domain							.811	
PLWD1, Perceived Work-Life Domain							.686	
PLWD4R, Perceived Work-Life Domain							.681	
RC4, Response Cost								.910
RC3, Response Cost								.903
RC2, Response Cost								.710

The EFA results for both PTS and PTV were positive. The Bartlett test of sphericity was statistically significant, and the MSA was .902, which exceeds the acceptable threshold of .50 (Hair et al., 2010), indicating that there are enough correlations among the variables.

Furthermore, the communalities for all items exceed .50 and are considered acceptable (Hair et al., 2010).

The pattern matrix shows that PTS1 had cross-loading on two components. Accordingly, PTS1 was dropped, resulting in high loading of the individual items on their variables, as shown in Table 9. There were no signs that items loaded on other variables, which provides confidence in the discriminant validity. Convergent validity was also checked; there were no indications that any items had less than 0.6 loadings on their related variables.

TABLE 9: PATTERN MATRIX – PTV AND PTS DROPPING PTS1.

	Component	
	1	2
PTV2, Perceived Threat Vulnerability	.893	
PTV4, Perceived Threat Vulnerability	.852	
PTV3, Perceived Threat Vulnerability	.822	
PTV1, Perceived Threat Vulnerability	.821	
PTS2, Perceived Threat Severity		.930
PTS4, Perceived Threat Severity		.873
PTS3, Perceived Threat Severity		.871

Next, an EFA was run for all factors except PTS and PTV. The Bartlett test of sphericity was statistically significant. The MSA also exceeded the acceptable threshold of .50 with a result of .805 (Hair et al., 2010). Therefore, there are enough correlations among the variables. Furthermore, with only two exceptions, the communalities for all items exceeded .50 (Hair et al., 2010) and are considered acceptable; the two exceptions are the fourth item used to measure Perceived Work-Life Domain (PLWD4R = .465) and the fourth item used to measure Perceived Behavioral Control (SE4 = .466). As stated above, they were retained as these items have been used in prior studies that proved their reliability and validity.

Finally, the pattern matrix (see Table 10) shows that all the items load on their respective variables. There are no signs that any items load on other variables, providing confidence in the discriminant validity. There are also no signs that any items load less than 0.6 on their related variables, indicating convergent validity.

After PTS1 was dropped, a reliability test was run for PTS without PTS1. This resulted in a Cronbach's alpha of .884, which is higher than the acceptable level of .70 (item reliability). The final reliability results for all of the variables are presented in Table 11.

TABLE 10: PATTERN MATRIX – WITHOUT PTV OR PTS

	Component						
	1	2	3	4	5	6	7
RWD3, Reward	.945						
RWD4, Reward	.944						
RWD2, Reward	.868						
RWD1, Reward	.728						
SR2, Scenario Realism		.915					
SR1, Scenario Realism		.893					
SR4, Scenario Realism		.869					
SR3, Scenario Realism		.840					
INT5R, Intention			.969				
INT4R, Intention			.940				
INT6R, Intention			.918				
RE2, Response Efficacy				.935			
RE1, Response Efficacy				.934			
RE4, Response Efficacy				.648			
RE3, Response Efficacy				.628			
SE1, Perceived Behavioral Control					.818		
SE3, Perceived Behavioral Control					.794		
SE2, Perceived Behavioral Control					.782		
SE4, Perceived Behavioral Control					.677		
PLWD2, Perceived Work-Life Domain						.859	
PLWD3R, Perceived Work-Life Domain						.810	
PLWD1, Perceived Work-Life Domain						.686	
PLWD4R, Perceived Work-Life Domain						.681	
RC4, Response Cost							.914
RC3, Response Cost							.908
RC2, Response Cost							.719

TABLE 11: RELIABILITY STATISTICS

Construct	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of Items
Scenario Realism (SR)	.893	.902	4
Perceived Work-life Domain (PLWD)	.756	.756	4
Perceived Self Efficacy (SE)	.750	.761	4
Perceived Threat Severity (PTS)	.884	.884	3
Perceived Threat Vulnerability (PTV)	.875	.876	4
Reward (RWD)	.894	.897	4
Response Efficacy (RE)	.829	.830	4
Response Cost (RC)	.797	.796	3
Intention (INTR)	.928	.928	3

5.1.4 Developing Summated Scales

As this study uses multiple regression analysis to test the two proposed models, it is critical to ensure that measurement error concerns are addressed. A summated scale can be used to address this (Hair et al., 2010); it is a key approach when dependency on a single item to measure a variable is reduced by the use of multiple items to measure this variable. According to Hair et al. (2010), summated scales are becoming more common in academic research as they increase the reliability of the measurement.

A summated scale can add value if the items used to represent the construct were good (Hair et al., 2010); that is, if they pass the empirical tests and there is theoretical justification for their use. As described in the previous sections, an EFA was used to empirically test the items in this study and provided the required assurance for the convergent validity and discriminant validity of the items. Further, in the reliability test (Table 11), all of the items passed the required threshold of .70 (Hair et al., 2010), indicating that a summated scale can be created.

Therefore, the requirements to create the summated scale were met. In a summated scale, the average of the different variables for each concept is used in the analysis (Hair et al., 2010). Accordingly, these averages were computed and a summated scale was developed for each concept.

5.1.5 Multiple Regression Analysis Assumptions

It is crucial to check the regression analysis assumptions prior to running the actual test. Hair et al. (2010) state that issues with normality, linearity, and homoscedasticity assumptions can affect and weaken the observed correlation. Multicollinearity should also be diagnosed to avoid any issues with the test (Hair et al., 2010). Therefore, we tested the normality of the variables in addition to checking for multicollinearity, linearity, and homoscedasticity. These tests were conducted for both models proposed in this paper.

5.1.5.1 Model 1 Assumptions

Beginning with Model 1, a visual examination was performed to check the normality, linearity, and constant variance of the error term assumptions. For this purpose, a histogram, a normal P-P plot, and a scatterplot for the residuals were generated from SPSS. A visual examination of the histogram and normal P-P plot can provide reasonable assurance that the variables are relatively normally distributed. Therefore, it was concluded that the normality assumption was

not violated in Model 1. A visual examination of the P-P plot also did not reveal any apparently nonlinear relationship. Therefore, it was concluded that the linearity assumption was not violated. A visual examination of the scatterplot did not reveal any signs of heteroscedasticity, so it was concluded that the constant variance of error term assumption was not violated.

Next, multicollinearity was tested for Model 1. Hair et al. (2010) state that multicollinearity can have a severe effect on the regression interpretation as it may reduce the overall R2, confuse the estimation of the regression coefficients, and negatively impact the statistical significance of the coefficient tests. Two key tables were produced to examine multicollinearity in Model 1: Table 12 shows the correlation, and Table 13 shows the VIT. As shown in Table 12, all of the variables have correlation values of less than 0.7 with each other, indicating that there are no issues with multicollinearity. The VIT table also shows that all variables have a VIF score below the threshold level suggested by Hair et al. (2010), indicating that there are no signs of multicollinearity.

After all the assumptions required for regression analysis were examined (normality, linearity, and homoscedasticity) and multicollinearity had been ruled out, it was determined that Model 1 was ready for the next step, the regression analysis.

TABLE 12: MODEL 1 – CORRELATIONS

	Perceived Work-life Domain (PLWD)	Gender	Age	Marital Status	Education	Experience	Position	Organization Size	Industry	Job Role	Tenure	IT Knowledge	Scenario Realism (SR)	Device Ownership (MCDevice)	Company Data Sensitivity (MCCData)	Personal Data Sensitivity (MCPData)	Employee's Location (MCPlace)	Activity Type (MCActivity)	Time of Activity (MCTime)
Perceived Work-life Domain (PLWD)	1	-0.007	0.004	-0.056	-0.047	0.04	-0.003	0.007	0.001	-0.005	0.032	0.019	0.05	0.148	-0.079	0.069	0.324	0.523	0.334
Gender	-0.007	1	0.044	-0.005	-0.158	0.052	0.18	0.008	-0.158	0.244	0.026	-0.232	-0.072	0.004	-0.001	-0.015	0.044	-0.044	0.058
Age	0.004	0.044	1	-0.285	-0.032	0.495	-0.152	-0.038	-0.045	0.087	0.266	-0.097	-0.044	-0.009	0.036	0.006	0.029	-0.046	0.009
Marital Status	-0.056	-0.005	-0.285	1	-0.106	-0.221	0.176	0.009	0.035	0.037	-0.168	-0.039	-0.023	-0.026	0.036	0.002	-0.004	-0.012	0.012
Education	-0.047	-0.158	-0.032	-0.106	1	-0.049	-0.219	0.034	-0.102	-0.105	-0.033	0.158	0.152	0.021	0.073	0.044	-0.014	-0.021	-0.06
Experience	0.04	0.052	0.495	-0.221	-0.049	1	-0.172	0.083	-0.022	0.079	0.419	0.017	0.026	-0.039	0.057	0.004	0.061	0.017	0.046
Position	-0.003	0.18	-0.152	0.176	-0.219	-0.172	1	0.14	-0.104	0.21	-0.18	-0.217	-0.084	-0.046	0.014	-0.011	0.016	-0.021	-0.004
Organization Size	0.007	0.008	-0.038	0.009	0.034	0.083	0.14	1	-0.058	0.02	0.14	0.021	-0.04	0.004	-0.006	-0.005	-0.021	0.024	-0.029
Industry	0.001	-0.158	-0.045	0.035	-0.102	-0.022	-0.104	-0.058	1	-0.178	-0.02	0.101	0.025	0.002	0.013	-0.02	0.009	-0.003	0.014
Job Role	-0.005	0.244	0.087	0.037	-0.105	0.079	0.21	0.02	-0.178	1	0.033	-0.38	-0.066	-0.032	0.054	-0.005	0.048	-0.028	0.037
Tenure	0.032	0.026	0.266	-0.168	-0.033	0.419	-0.18	0.14	-0.02	0.033	1	0.012	0.018	-0.046	0.02	-0.014	0.024	0.025	0.034
IT Knowledge	0.019	-0.232	-0.097	-0.039	0.158	0.017	-0.217	0.021	0.101	-0.38	0.012	1	0.132	0.021	-0.048	-0.018	0.013	0.009	0.002
Scenario Realism (SR)	0.05	-0.072	-0.044	-0.023	0.152	0.026	-0.084	-0.04	0.025	-0.066	0.018	0.132	1	0.073	0.01	0.023	-0.021	-0.055	-0.013
Device Ownership (MCDevice)	0.148	0.004	-0.009	-0.026	0.021	-0.039	-0.046	0.004	0.002	-0.032	-0.046	0.021	0.073	1	-0.209	0.204	0.085	0.16	0.116
Company Data Sensitivity (MCCData)	-0.079	-0.001	0.036	0.036	0.073	0.057	0.014	-0.006	0.013	0.054	0.02	-0.048	0.01	-0.209	1	0.175	-0.066	-0.075	-0.071
Personal Data Sensitivity (MCPData)	0.069	-0.015	0.006	0.002	0.044	0.004	-0.011	-0.005	-0.02	-0.005	-0.014	-0.018	0.023	0.204	0.175	1	0.062	0.046	0.099
Employee's Location (MCPlace)	0.324	0.044	0.029	-0.004	-0.014	0.061	0.016	-0.021	0.009	0.048	0.024	0.013	-0.021	0.085	-0.066	0.062	1	0.25	0.601
Activity Type (MCActivity)	0.523	-0.044	-0.046	-0.012	-0.021	0.017	-0.021	0.024	-0.003	-0.028	0.025	0.009	-0.055	0.16	-0.075	0.046	0.25	1	0.298
Time of Activity (MCTime)	0.334	0.058	0.009	0.012	-0.06	0.046	-0.004	-0.029	0.014	0.037	0.034	0.002	-0.013	0.116	-0.071	0.099	0.601	0.298	1

TABLE 13: MODEL 1 – VIF

Variables	Collinearity Statistics	
	Tolerance	VIF
Gender	.871	1.148
Age	.691	1.447
Marital Status	.876	1.142
Education	.859	1.164
Experience	.641	1.561
Position	.788	1.268
Organization Size	.928	1.078
Industry	.920	1.087
Job Role	.790	1.265
Tenure	.784	1.276
IT Knowledge	.790	1.265
Scenario Realism (SR)	.946	1.057
Device Ownership (MCDevice)	.866	1.155
Company Data Sensitivity (MCCData)	.886	1.129
Personal Data Sensitivity (MCPData)	.899	1.113
Employee's Location (MCPlace)	.628	1.594
Activity Type (MCActivity)	.872	1.147
Time of Activity (MCTime)	.604	1.654

5.1.5.2 Model 2 Assumptions

The same approach as that used with Model 1 was used to test the assumptions of normality, linearity, and constant variance of error terms for Model 2. In this case, a visual examination of the histogram of residuals did not clearly indicate that the normality assumptions were met. According to Hair et al. (2010), normality impacts the validity of the results of the statistical tests. This effect becomes more apparent when the sample is smaller than 200. However, when the sample size exceeds 200, the impact of normality diminishes (Hair et al., 2010). Therefore, in this study, with a sample size of 3035, it was decided to proceed with the regression analysis but to interpret the results with caution. A visual examination of the P-P plot showed that there were signs of a relatively linear relationship, so it was concluded that the linearity assumption was sufficient. Finally, a visual examination of the scatterplot did not reveal any signs of heteroscedasticity, so it was concluded that the constant variance of error terms assumption was not violated.

Before proceeding with the regression analysis, multicollinearity was examined for Model 2. Table 14 shows the correlations for Model 2; no correlation between different variables exceeds 0.7. Further, the results of the VIT score (shown in Table 15) are all below the threshold level. Therefore, it was concluded that there were no signs of multicollinearity.

TABLE 14: MODEL 2 – CORRELATIONS

	Intention (INTR)	Gender	Age	Marital Status	Education	Experience	Position	Organization Size	Industry	Job Role	Tenure	IT Knowledge	Scenario Realism (SR)	Perceived Threat Severity (PTS)	Perceived Threat Vulnerability (PTV)	Reward (RWD)	Response Efficacy (RE)	Response Cost (RC)	Perceived Self Efficacy (SE)
Intention (INTR)	1	0.152	0.111	-0.032	-0.086	0.128	0.018	0.003	0.002	0.043	0.081	-0.013	0.007	0.296	0.312	-0.094	0.314	0.103	0.282
Gender	0.152	1	0.044	-0.005	-0.158	0.052	0.18	0.008	-0.158	0.244	0.026	-0.232	-0.072	0.13	0.115	-0.155	0.109	0.041	0.113
Age	0.111	0.044	1	-0.285	-0.032	0.495	-0.152	-0.038	-0.045	0.087	0.266	-0.097	-0.044	0.116	0.147	-0.009	0.142	0.101	0.077
Marital Status	-0.032	-0.005	-0.285	1	-0.106	-0.221	0.176	0.009	0.035	0.037	-0.168	-0.039	-0.023	0.022	-0.075	-0.134	-0.086	-0.05	-0.033
Education	-0.086	-0.158	-0.032	-0.106	1	-0.049	-0.219	0.034	-0.102	-0.105	-0.033	0.158	0.152	-0.08	-0.06	0.044	-0.045	0.042	-0.098
Experience	0.128	0.052	0.495	-0.221	-0.049	1	-0.172	0.083	-0.022	0.079	0.419	0.017	0.026	0.136	0.145	-0.117	0.136	0.085	0.089
Position	0.018	0.18	-0.152	0.176	-0.219	-0.172	1	0.14	-0.104	0.21	-0.18	-0.217	-0.084	0.032	-0.035	-0.184	-0.06	-0.051	-0.008
Organization Size	0.003	0.008	-0.038	0.009	0.034	0.083	0.14	1	-0.058	0.02	0.14	0.021	-0.04	0.057	0.077	-0.071	0.058	0.065	0.002
Industry	0.002	-0.158	-0.045	0.035	-0.102	-0.022	-0.104	-0.058	1	-0.178	-0.02	0.101	0.025	-0.023	-0.001	0.135	0.001	-0.021	0.013
Job Role	0.043	0.244	0.087	0.037	-0.105	0.079	0.21	0.02	-0.178	1	0.033	-0.38	-0.066	0.059	-0.004	-0.178	-0.041	-0.018	0.006
Tenure	0.081	0.026	0.266	-0.168	-0.033	0.419	-0.18	0.14	-0.02	0.033	1	0.012	0.018	0.094	0.117	-0.015	0.117	0.057	0.072
IT Knowledge	-0.013	-0.232	-0.097	-0.039	0.158	0.017	-0.217	0.021	0.101	-0.38	0.012	1	0.132	0.025	0.089	0.124	0.085	0.066	0.048
Scenario Realism (SR)	0.007	-0.072	-0.044	-0.023	0.152	0.026	-0.084	-0.04	0.025	-0.066	0.018	0.132	1	0.132	0.121	0.003	0.151	0.07	0.122
Perceived Threat Severity (PTS)	0.296	0.13	0.116	0.022	-0.08	0.136	0.032	0.057	-0.023	0.059	0.094	0.025	0.132	1	0.615	-0.112	0.462	0.239	0.375
Perceived Threat Vulnerability (PTV)	0.312	0.115	0.147	-0.075	-0.06	0.145	-0.035	0.077	-0.001	-0.004	0.117	0.089	0.121	0.615	1	0.138	0.669	0.316	0.476
Reward (RWD)	-0.094	-0.155	-0.009	-0.134	0.044	-0.117	-0.184	-0.071	0.135	-0.178	-0.015	0.124	0.003	-0.112	0.138	1	0.156	0.069	0.017
Response Efficacy (RE)	0.314	0.109	0.142	-0.086	-0.045	0.136	-0.06	0.058	0.001	-0.041	0.117	0.085	0.151	0.462	0.669	0.156	1	0.341	0.563
Response Cost (RC)	0.103	0.041	0.101	-0.05	0.042	0.085	-0.051	0.065	-0.021	-0.018	0.057	0.066	0.07	0.239	0.316	0.069	0.341	1	0.276
Perceived Self Efficacy (SE)	0.282	0.113	0.077	-0.033	-0.098	0.089	-0.008	0.002	0.013	0.006	0.072	0.048	0.122	0.375	0.476	0.017	0.563	0.276	1

TABLE 15: MODEL 2 – VIF

Variables	Collinearity Statistics	
	Tolerance	VIF
Gender	.847	1.180
Age	.684	1.461
Marital status	.859	1.164
Education	.857	1.167
Experience	.629	1.590
Position	.779	1.284
Organization Size	.918	1.090
Industry	.915	1.093
Job Role	.787	1.271
Tenure	.784	1.275
IT Knowledge	.783	1.277
Scenario Realism (SR)	.920	1.086
Perceived Threat Severity (PTS)	.563	1.776
Perceived Threat Vulnerability (PTV)	.408	2.449
Reward (RWD)	.809	1.236
Response Efficacy (RE)	.450	2.225
Response Cost (RC)	.850	1.176
Perceived Self Efficacy (SE)	.641	1.559

The tests conducted on Model 2 to examine the assumptions required for regression analysis (normality, linearity, and homoscedasticity) did not indicate any presence of multicollinearity. It was therefore concluded that Model 2 was ready for the next step, the regression analysis.

5.2 Testing Research Model 1

In the next step, a regression analysis was conducted on Model 1. The control variables were entered into the regression analysis first, and then the remaining variables were entered to capture the impact of the control variables. First, the validity of the model was checked. In the ANOVA results (see Table 17), the p-value is less than .05, so the null hypothesis was rejected in favor of the alternative hypothesis. Therefore, there is good reason to infer that the model is valid.

Following the recommendations of Hankins, French, and Horne (2000), the adjusted R2 was used to interpret the results of the regression analysis. As shown in Table 16, the adjusted R2 was .331. This means that 33.1% of the variation in the dependent variable (i.e., Perceived Work-Life Domain) is explained by the independent variables (i.e., BOYD contextual factors and the control variables). However, 66.9% of the variation in the dependent variable remains

unexplained. Of Model 1's explanatory power of 33.1%, 0.7% results from the control variables, while the remaining 33.1% is the effect of BOYD contextual factors.

TABLE 16: MODEL 1 SUMMARY

Model	R	R Squared	Adjusted R Squared	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
Control Variables	.105	.011	.007	1.45466	.011	2.802	12	3022	.001
Full Model	.579	.335	.331	1.19411	.324	244.784	6	3016	.000

TABLE 17: MODEL 1 ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
Control Variables	Regression	71.150	12	5.929	2.802	.001
	Residual	6394.693	3022	2.116		
	Total	6465.843	3034			
Full Model	Regression	2165.361	18	120.298	84.367	.000
	Residual	4300.481	3016	1.426		
	Total	6465.843	3034			

The coefficient results presented in Table 18 enable an examination of the effect of each independent and control variable on the dependent variable and the significance of those effects. Of the control variables, only marital state, education, and scenario realism had a significant impact on the dependent variable; the other control variables were insignificant. Marital state had a negative effect of -.051 on the dependent variable. Education had a negative effect of -.045. However, scenario realism had a positive effect of .082 on the dependent variable.

An examination of the BYOD contextual factors showed that device ownership had a significant effect of .036 on the dependent variable. Therefore, H1 is supported. Similarly, employee location had a significant effect of .142 on the dependent variable, supporting H2. H3 is also supported: Time of activity had a significant effect of .106 on the dependent variable. Furthermore, activity type had a significant effect of .451; therefore, H4 is supported. However, both company data sensitivity and personal data sensitivity were insignificant. Accordingly, H5a and H5b are not supported.

Figure 8 illustrates the overall explanatory power of Model 1, the significance of the relationship of each variable with the dependent variable, and the effects of each of these relationships based on the results of the regression analysis.

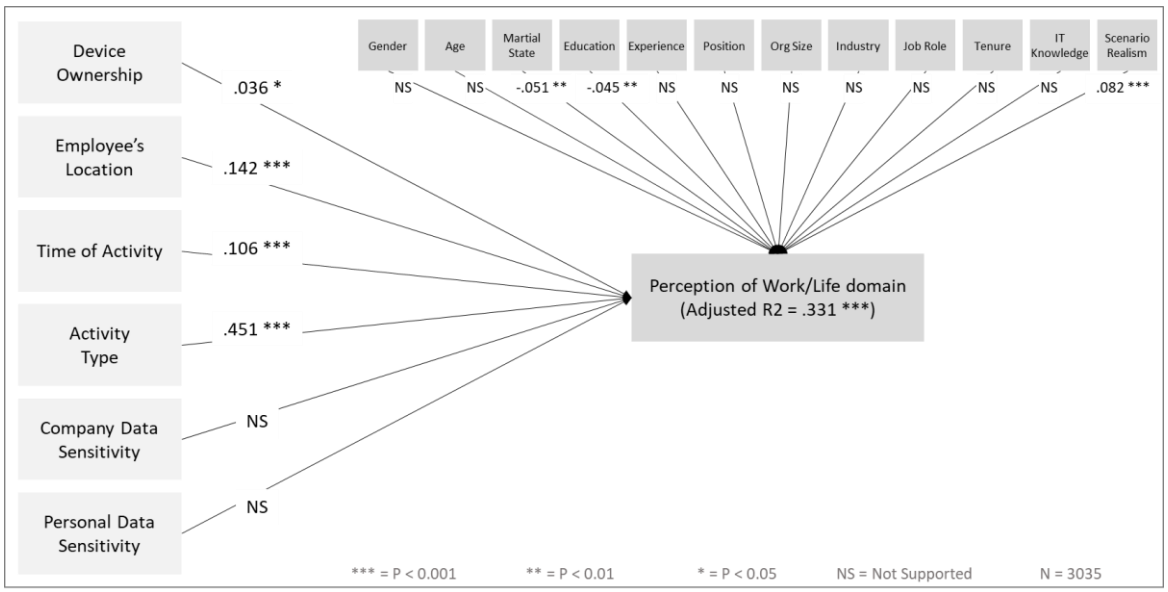


FIGURE 8: MODEL 1 – RESULTS SUMMARY

TABLE 18: MODEL 1 COEFFICIENTS

Model			Standardized Coefficients			Correlations			Collinearity Statistics	
		Std. Error	Beta	t	Sig.	Zero-Order	Partial	Part	Tolerance	VIF
Control Variables	(Constant)	.341		12.559	.000					
	Gender	.057	-.013	-.693	.488	-.007	-.013	-.013	.878	1.139
	Age	.031	-.029	-1.334	.182	.004	-.024	-.024	.695	1.438
	Marital Status	.015	-.061	-3.149	.002	-.056	-.057	-.057	.880	1.137
	Education	.034	-.064	-3.312	.001	-.047	-.060	-.060	.871	1.148
	Experience	.028	.031	1.390	.165	.040	.025	.025	.646	1.548
	Rank	.047	.006	.310	.757	-.003	.006	.006	.792	1.263
	Org Size	.015	.004	.234	.815	.007	.004	.004	.931	1.075
	Org Ind	.006	-.008	-.419	.675	.001	-.008	-.008	.923	1.083
	Role	.070	-.001	-.035	.972	-.005	-.001	-.001	.794	1.259
	Tenure	.028	.014	.676	.499	.032	.012	.012	.786	1.272
	IT Knowledge	.023	.015	.738	.461	.019	.013	.013	.794	1.260
	Scenario Realism (SR)	.020	.054	2.903	.004	.050	.053	.053	.956	1.046
Full Model	(Constant)	.316		.628	.530					
	Gender	.047	-.003	-.207	.836	-.007	-.004	-.003	.871	1.148
	Age	.026	.011	.616	.538	.004	.011	.009	.691	1.447
	Marital Status	.012	-.051	-3.222	.001	-.056	-.059	-.048	.876	1.142
	Education	.028	-.045	-2.824	.005	-.047	-.051	-.042	.859	1.164
	Experience	.023	.001	.052	.958	.040	.001	.001	.641	1.561
	Rank	.039	.017	1.031	.303	-.003	.019	.015	.788	1.268
	Org Size	.012	.004	.271	.786	.007	.005	.004	.928	1.078
	Org Ind	.005	-.003	-.221	.825	.001	-.004	-.003	.920	1.087
	Role	.058	.001	.046	.963	-.005	.001	.001	.790	1.265
	Tenure	.023	.004	.216	.829	.032	.004	.003	.784	1.276
	IT Knowledge	.019	.010	.620	.535	.019	.011	.009	.790	1.265
	Scenario Realism (SR)	.017	.082	5.365	.000	.050	.097	.080	.946	1.057
	Device Ownership (MCDevice)	.082	.036	2.243	.025	.148	.041	.033	.866	1.155
	Company Data Sensitivity (MCCData)	.047	-.022	-1.374	.169	-.079	-.025	-.020	.886	1.129
	Personal Data Sensitivity (MCPData)	.054	.026	1.658	.097	.069	.030	.025	.899	1.113
	Employee's Location (MCPlace)	.064	.142	7.559	.000	.324	.136	.112	.628	1.594
	Activity Type (MCActivity)	.047	.451	28.328	.000	.523	.458	.421	.872	1.147
	Time of Activity (MCTime)	.060	.106	5.530	.000	.334	.100	.082	.604	1.654

5.3 Testing Research Model 2

5.3.1 Cases Categorization and Approach

In order to test Model 2, the respondents were first categorized into three groups. The first contained respondents who perceived the scenario as a life domain, the second those who perceived the scenario as a work domain, and the final group those who found it difficult to determine which domain the scenario fell into and described it as a gray area. Four hundred and ninety-four respondents perceived the scenario as a life domain; 940 considered it a work domain, and 1601 viewed it as a gray area.

Model 2 was tested using a similar approach to that used with Model 1. First, the control variables were entered into the regression analysis, and then the remaining variables were entered to capture the impact of the control variables. However, for Model 2, three regression analyses were conducted, one for each domain group.

5.3.2 Testing Effect of Being in Life Domain on Information Security Behaviors

The ANOVA results for the first group, the life domain (shown in Table 20) support the validity of the model. Since the p-value is less than .05, the null hypothesis was rejected in favor of the alternative hypothesis, and it can be inferred that the model is valid.

The adjusted R2 shown in Table 19 is .181. This indicates that, for the life domain group, 18.1% of the variation in the dependent variable (i.e., intention to comply with the information security policy) is explained by the independent variables (i.e., the PMT variables and control variables); 81.9% of the variation in the dependent variable remains unexplained. Of this 18.1%, 6.3% of the variation in the dependent variable results from the control variables, while the remaining 11.8% is the effect of the PMT variables.

TABLE 19: MODEL 2 – LIFE DOMAIN SUMMARY

Model	R		R Square	Adjusted R Squared	Std. Error of the Estimate	Change Statistics					Durbin–Watson Statistic	
	LWDG = 1 (Selected)	LWDG ≈ 1 (Unselected)				R Squared Change	F Change	df1	df2	Sig. F Change	LWDG = 1 (Selected)	LWDG ≈ 1 (Unselected)
Control Variables	.293		.086	.063	1.53126	.086	3.759	12	481	.000		
Full Model	.460	.328	.211	.181	1.43124	.126	12.596	6	475	.000	2.061	1.988

TABLE 20: MODEL 2 – LIFE DOMAIN ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
Control Variables	Regression	105.774	12	8.814	3.759	.000
	Residual	1127.832	481	2.345		
	Total	1233.605	493			
Full Model	Regression	260.593	18	14.477	7.067	.000
	Residual	973.012	475	2.048		
	Total	1233.605	493			

Figure 9 shows the results of the regression analysis for Model 2 for the life domain group. The figure demonstrates the overall explanatory power of Model 2, the significant relationship of each variable to the dependent variables, and effect of each of these relationships.

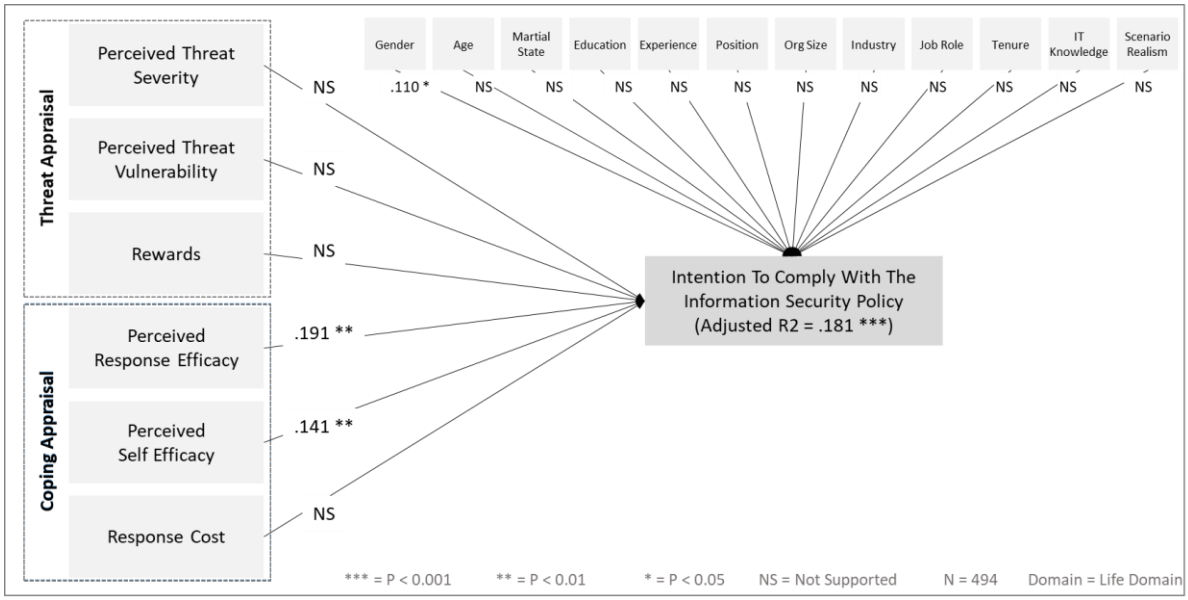


FIGURE 9: MODEL 2 – LIFE DOMAIN RESULT SUMMARY

TABLE 21: MODEL 2 – LIFE DOMAIN COEFFICIENTS

Model			Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics	
		Std. Error	Beta			Zero order	Partial	Part	Tolerance	VIF
Control Variables	(Constant)	.948		5.247	.000					
	Gender	.158	.163	3.385	.001	.201	.153	.148	.824	1.213
	Age	.078	.079	1.399	.162	.116	.064	.061	.595	1.682
	Marital Status	.039	-.074	-1.571	.117	-.097	-.071	-.068	.865	1.157
	Education	.088	-.034	-.731	.465	-.093	-.033	-.032	.886	1.128
	Experience	.081	-.021	-.352	.725	.070	-.016	-.015	.550	1.818
	Rank	.120	.094	1.937	.053	.083	.088	.084	.802	1.247
	Org Size	.039	.050	1.076	.282	.082	.049	.047	.887	1.127
	Org Industry	.017	-.012	-.256	.798	-.058	-.012	-.011	.875	1.143
	Role	.195	-.088	-1.828	.068	-.018	-.083	-.080	.817	1.224
	Tenure	.075	.056	1.106	.269	.084	.050	.048	.736	1.359
	IT Knowledge	.059	.009	.174	.862	-.058	.008	.008	.751	1.331
	Scenario Realism (SR)	.051	-.111	-2.448	.015	-.149	-.111	-.107	.920	1.087
Full Model	(Constant)	1.064		.696	.487					
	Gender	.150	.110	2.422	.016	.201	.110	.099	.800	1.250
	Age	.074	.044	.831	.406	.116	.038	.034	.582	1.717
	Marital Status	.037	-.065	-1.473	.141	-.097	-.067	-.060	.857	1.167
	Education	.083	-.002	-.056	.955	-.093	-.003	-.002	.870	1.149
	Experience	.076	-.045	-.824	.410	.070	-.038	-.034	.545	1.836
	Rank	.115	.085	1.831	.068	.083	.084	.075	.773	1.294
	Org Size	.037	.046	1.055	.292	.082	.048	.043	.867	1.153
	Org Industry	.016	-.002	-.036	.972	-.058	-.002	-.001	.863	1.159
	Role	.187	-.031	-.675	.500	-.018	-.031	-.028	.779	1.284
	Tenure	.071	.032	.669	.504	.084	.031	.027	.728	1.374
	IT Knowledge	.056	-.012	-.264	.792	-.058	-.012	-.011	.745	1.343
	Scenario Realism (SR)	.048	-.075	-1.743	.082	-.149	-.080	-.071	.901	1.110
	Perceived Threat Severity (PTS)	.104	.050	.948	.344	.247	.043	.039	.598	1.671
	Perceived Threat Vulnerability (PTV)	.090	.074	1.202	.230	.323	.055	.049	.433	2.307
	Reward (RWD)	.047	.060	1.372	.171	.100	.063	.056	.858	1.165
	Response Efficacy (RE)	.093	.191	3.176	.002	.374	.144	.129	.459	2.177
	Response Cost (RC)	.053	-.019	-.422	.673	.173	-.019	-.017	.791	1.265
	Self Efficacy (SE)	.079	.141	2.877	.004	.313	.131	.117	.691	1.447

5.3.3 Testing Effect of Being in Gray Area on Information Security Behaviors

The results of the ANOVA for the gray area group are shown in Table 23. The ANOVA p-value is less than .05, so the null hypothesis was rejected in favor of the alternative hypothesis. Accordingly, the model is inferred to be valid. Since the model is valid, the adjusted R2 was then examined. Table 22 shows that the adjusted R2 for the entire model is .113 while the R2 for only the control variables is .046. This indicates that, for the gray area group, 11.3% of the variation in the dependent variable is explained by the independent variables, but 88.7% remains unexplained. Of the 11.3%, 4.6% in the variation of the dependent variable results from the control variables, while the remaining 6.7% is caused by the PMT variables.

The coefficients for the gray area domain group of Model 2 (Table 24) show that gender is the only control variable that has a significant impact on the dependent variable, with an effect size of .072. However, all of the PMT variables are significant. Perceived threat severity had an effect of .092 on the dependent variable, perceived threat vulnerability an effect of .129, and perceived response efficacy an effect of .126. Response cost had an effect of .079 on the dependent variable. However, reward and perceived self-efficacy had negative effects on the dependent variable: -.166 and -.073, respectively. Figure 10 shows the results of the gray area domain of Model 2.

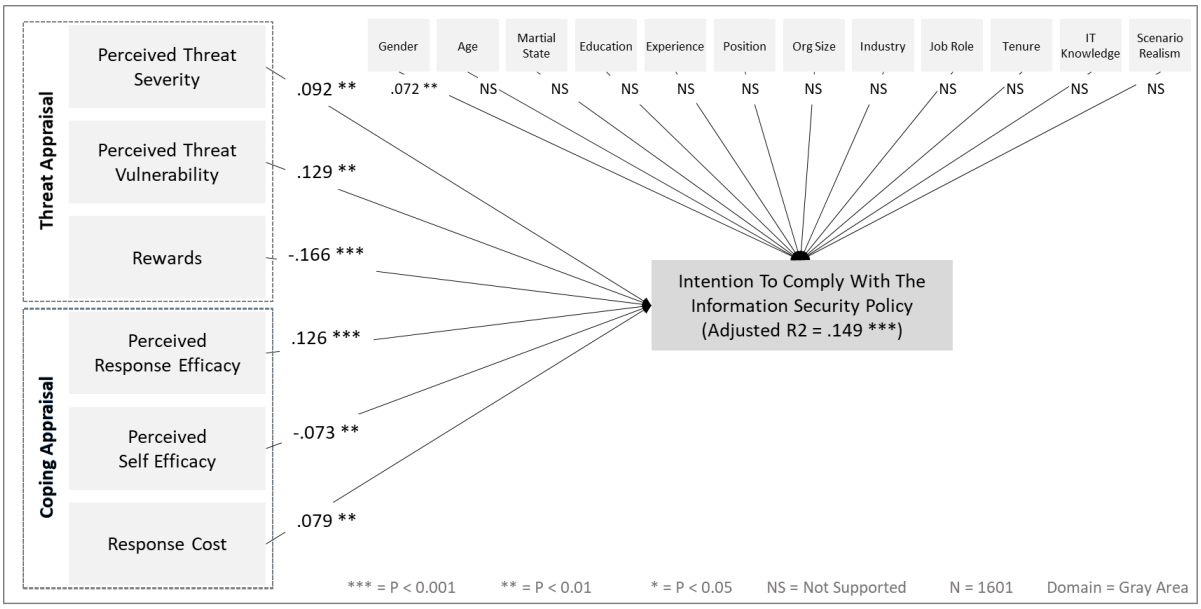


FIGURE 10: MODEL 2 – GRAY DOMAIN RESULT SUMMARY

TABLE 22: MODEL 2 – GRAY DOMAIN SUMMARY

Model Summary												
Model	R		R Squared	Adjusted R Squared	Std. Error of the Estimate	Change Statistics					Durbin–Watson Statistic	
	LWDG = 2 (Selected)	LWDG ≈ 2 (Unselected)				R Squared Change	F Change	df1	df2	Sig. F Change	LWDG = 2 (Selected)	LWDG ≈ 2 (Unselected)
Control Variables	.213		.046	.038	1.78379	.046	6.312	12	1588	.000		
Full Model	.398	.343	.158	.149	1.67829	.113	35.320	6	1582	.000	2.036	1.953

TABLE 23: MODEL 2 – GRAY DOMAIN ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
Control Variables	Regression	241.028	12	20.086	6.312	.000
	Residual	5052.856	1588	3.182		
	Total	5293.884	1600			
Full Model	Regression	837.930	18	46.552	16.527	.000
	Residual	4455.954	1582	2.817		
	Total	5293.884	1600			

TABLE 24: MODEL 2 – GRAY DOMAIN COEFFICIENTS

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Zero-order	Partial	Part	Tolerance	VIF
Control Variables	(Constant)	3.193	.571		5.591	.000					
	Gender	.532	.096	.145	5.509	.000	.157	.137	.135	.870	1.150
	Age	.088	.055	.046	1.586	.113	.087	.040	.039	.709	1.411
	Marital Status	.010	.025	.010	.396	.692	-.008	.010	.010	.858	1.166
	Education	-.132	.058	-.061	-2.279	.023	-.087	-.057	-.056	.829	1.207
	Experience	.140	.045	.095	3.120	.002	.128	.078	.077	.650	1.539
	Rank	-.001	.081	.000	-.010	.992	.020	.000	.000	.758	1.319
	Org Size	.008	.026	.007	.291	.771	.013	.007	.007	.936	1.068
	Org Industry	.004	.011	.009	.374	.709	-.006	.009	.009	.935	1.070
	Role	.014	.115	.003	.125	.900	.059	.003	.003	.790	1.266
	Tenure	.009	.046	.006	.201	.841	.061	.005	.005	.770	1.299
	IT Knowledge	-.008	.039	-.006	-.217	.828	-.049	-.005	-.005	.778	1.285
	Scenario Realism (SR)	.052	.035	.038	1.493	.136	.011	.037	.037	.936	1.069
Full Model	(Constant)	2.121	.592		3.586	.000					
	Gender	.265	.093	.072	2.850	.004	.157	.071	.066	.832	1.201
	Age	.019	.052	.010	.369	.712	.087	.009	.009	.697	1.435
	Marital Status	-.018	.024	-.018	-.725	.469	-.008	-.018	-.017	.824	1.213
	Education	-.080	.055	-.037	-1.465	.143	-.087	-.037	-.034	.820	1.220
	Experience	.075	.043	.051	1.744	.081	.128	.044	.040	.628	1.591
	Rank	-.045	.077	-.016	-.587	.557	.020	-.015	-.014	.745	1.343
	Org Size	-.019	.025	-.018	-.757	.449	.013	-.019	-.017	.920	1.086
	Org Industry	.010	.010	.024	.979	.328	-.006	.025	.023	.919	1.089
	Role	-.043	.109	-.010	-.391	.696	.059	-.010	-.009	.780	1.281
	Tenure	-.010	.043	-.006	-.222	.825	.061	-.006	-.005	.767	1.304
	IT Knowledge	-.045	.037	-.032	-1.214	.225	-.049	-.031	-.028	.766	1.306
	Scenario Realism (SR)	-.052	.033	-.038	-1.562	.118	.011	-.039	-.036	.883	1.132
	Perceived Threat Severity (PTS)	.146	.051	.092	2.831	.005	.283	.071	.065	.505	1.979
	Perceived Threat Vulnerability (PTV)	.207	.060	.129	3.446	.001	.272	.086	.079	.379	2.642
	Reward (RWD)	-.171	.027	-.166	-6.256	.000	-.166	-.155	-.144	.753	1.329
	Response Efficacy (RE)	.217	.061	.126	3.546	.000	.257	.089	.082	.424	2.361
	Response Cost (RC)	-.102	.036	-.073	-2.823	.005	.046	-.071	-.065	.800	1.250
	Self Efficacy (SE)	.141	.053	.079	2.653	.008	.237	.067	.061	.596	1.677

5.3.4 Testing Effect of Being in Work Domain on Information Security Behaviors

Finally, for the work domain responses, the model was valid; the ANOVA result (Table 26) had a p-value below .05. The adjusted R2 (Table 25) was .157. This indicates that for the work domain group of Model 2, the independent variables account for 15.7% of variation in the dependent variable, while 84.3% remains unexplained. Of this, 15.7%, 3.7% of the variation in the dependent variable results from the control variables, while the remaining 12% is the effect of the PMT variables.

TABLE 25: MODEL 2 – WORK DOMAIN SUMMARY

Model	R		R Squared	Adjusted R Squared	Std. Error of the Estimate	Change Statistics					Durbin–Watson Statistic	
	LWDG = 3 (Selected)	LWDG ≈ 3 (Unselected)				R Squared Change	F Change	df1	df2	Sig. F Change	LWDG = 3 (Selected)	LWDG ≈ 3 (Unselected)
Control Variables	.223		.050	.037	1.56811	.050	4.040	12	927	.000		
Full Model	.416	.350	.173	.157	1.46763	.123	22.880	6	921	.000	2.086	1.911

TABLE 26: MODEL 2 - WORK DOMAIN ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
Control Variables	Regression	119.205	12	9.934	4.040	.000
	Residual	2279.475	927	2.459		
	Total	2398.680	939			
Full Model	Regression	414.895	18	23.050	10.701	.000
	Residual	1983.785	921	2.154		
	Total	2398.680	939			

The coefficients (Table 27) show that the organization's size and industry are significant; organization size had a negative effect of -.067 on the dependent variable, and industry had a positive effect of .065. However, none of the other control variables are significant. Of the PMT variables, reward and response cost were found to be insignificant. Perceived threat severity had a significant effect of .119 on the intention to comply with the information security policy. Similarly, perceived threat vulnerability had a significant effect of .101 on the dependent variable, and perceived response efficacy a significant effect of .150 on the dependent variable. Finally, perceived self-efficacy also had a significant effect of .116 on the dependent variable. Figure 11 summarizes the findings of the regression analysis for the work domain group of Model 2.

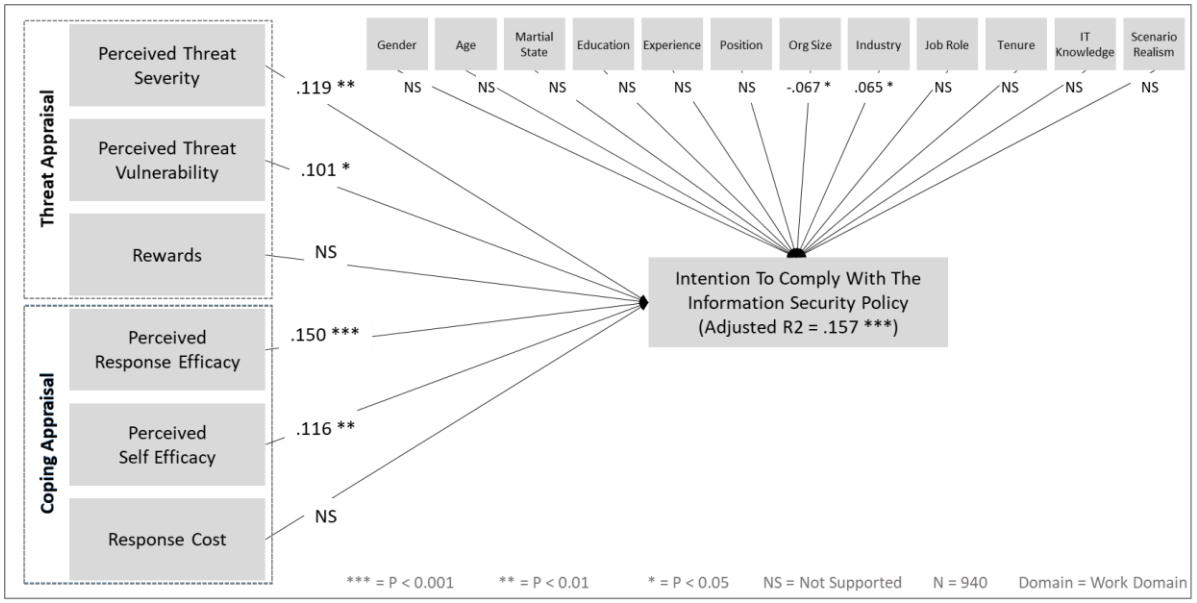


FIGURE 11: MODEL 2 – WORK DOMAIN RESULT SUMMARY

TABLE 27: MODEL 2 – WORK DOMAIN COEFFICIENTS

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations			Collinearity Statistics	
		B	Std. Error	Beta			Zero-order	Partial	Part	Tolerance	VIF
Control Variables	(Constant)	3.068	.681		4.503	.000					
	Gender	.384	.110	.118	3.483	.001	.103	.114	.112	.900	1.111
	Age	.124	.060	.079	2.067	.039	.114	.068	.066	.710	1.409
	Marital Status	.025	.029	.029	.849	.396	-.016	.028	.027	.899	1.113
	Education	-.064	.066	-.032	-.966	.334	-.056	-.032	-.031	.906	1.104
	Experience	.080	.057	.054	1.409	.159	.108	.046	.045	.688	1.453
	Rank	-.034	.091	-.013	-.370	.711	-.037	-.012	-.012	.822	1.216
	Org Size	-.048	.029	-.056	-1.673	.095	-.059	-.055	-.054	.921	1.085
	Industry	.027	.013	.072	2.138	.033	.057	.070	.068	.905	1.105
	Role	.156	.140	.041	1.121	.263	.021	.037	.036	.779	1.284
	Tenure	.089	.057	.055	1.561	.119	.090	.051	.050	.839	1.192
	IT Knowledge	.135	.044	.109	3.076	.002	.071	.101	.098	.820	1.220
	Scenario Realism (SR)	.003	.040	.002	.069	.945	.006	.002	.002	.970	1.031
Full Model	(Constant)	-1.036	.770		-1.345	.179					
	Gender	.187	.105	.057	1.788	.074	.103	.059	.054	.875	1.143
	Age	.064	.057	.041	1.129	.259	.114	.037	.034	.696	1.437
	Marital Status	.019	.027	.023	.716	.474	-.016	.024	.021	.892	1.122
	Education	.060	.063	.030	.946	.345	-.056	.031	.028	.872	1.147
	Experience	.052	.054	.035	.968	.333	.108	.032	.029	.672	1.487
	Rank	-.043	.086	-.017	-.501	.616	-.037	-.017	-.015	.807	1.239
	Org Size	-.059	.027	-.067	-2.146	.032	-.059	-.071	-.064	.909	1.100
	Industry	.025	.012	.065	2.051	.041	.057	.067	.061	.898	1.113
	Role	.083	.131	.021	.630	.529	.021	.021	.019	.770	1.298
	Tenure	.077	.053	.047	1.443	.149	.090	.048	.043	.837	1.195
	IT Knowledge	.074	.042	.060	1.777	.076	.071	.058	.053	.801	1.249
	Scenario Realism (SR)	-.067	.039	-.054	-1.748	.081	.006	-.058	-.052	.939	1.065
	Perceived Threat Severity (PTS)	.236	.070	.119	3.351	.001	.255	.110	.100	.718	1.394
	Perceived Threat Vulnerability (PTV)	.177	.074	.101	2.384	.017	.304	.078	.071	.499	2.005
	Reward (RWD)	-.043	.031	-.045	-1.379	.168	.013	-.045	-.041	.853	1.172
	Response Efficacy (RE)	.253	.069	.150	3.650	.000	.318	.119	.109	.528	1.894
	Response Cost (RC)	.040	.033	.037	1.201	.230	.134	.040	.036	.921	1.086
	Self Efficacy (SE)	.198	.060	.116	3.323	.001	.263	.109	.100	.740	1.351

5.3.5 Results of Model 2 Hypothesis

In order to examine research hypotheses 6 to 11, which were the basis for Model 2, Table 28 was generated from the results of the regression analyses for all three sample groups. The table compares the effects of the independent variables from protection motivation theory on the intention to comply with the information security policy (the dependent variable) for each sample group. The effects of perceived threat severity and perceived threat vulnerability on the dependent variable differ across the sample groups. These effects were significant for the gray

area and work domain groups but insignificant for the life domain group; therefore, H6 and H7 are supported. H8 and H11 are also supported: Both rewards and response cost were only significant for the gray area domain group; their effects were insignificant for the other two groups. Perceived self-efficacy remained significant for all groups, but the direction of its effect changed for the gray area domain group, supporting H10. H9 was not supported. The effect of perceived response efficacy remained significant and unchanged for all three domain groups.

TABLE 28: MODEL 2 – HYPOTHESIS RESULTS

	Life		Gray		Work		Hypotheses
	Significance	Effect Size	Significance	Effect Size	Significance	Effect Size	
Perceived Threat Severity (PTS)	NS	NS	P < .01	.092	P < .01	.119	H6: supported
Perceived Threat Vulnerability (PTV)	NS	NS	P < .01	.129	P < .05	.101	H7: supported
Reward (RWD)	NS	NS	P < .001	-.166	NS	NS	H8: supported
Response Efficacy (RE)	P < .01	.191	P < .001	.126	P < .001	.150	H9: not supported
Self Efficacy (SE)	P < .01	.141	P < .01	-.073	P < .01	.116	H10: supported
Response Cost (RC)	NS	NS	P < .01	.079	NS	NS	H11: supported

5.4 Chapter Summary

This chapter presented the approach to and results from analyzing the collected data. First, the data were screened and treated for any missing values. All the items used for the two models of this study were checked for reliability, and only those with high reliability were used in the analysis. In addition, exploratory factor analysis was performed on the items to ensure their convergent and discernment validity. Once the validity and reliability of items had been assured, a summated scale was developed to reduce the risk of any measurement error. After that, both models were tested using multiple regression analysis. The result of the test showed that all the hypotheses were supported except for H5a, H5b, and H9 as shown in Table 29. The results are discussed in the next chapter.

TABLE 29: HYPOTHESIS RESULTS

No	Hypothesis	Supported
H1:	Device ownership (i.e., whether owned by the employee or the organization) impacts employees' perceptions of whether they are in the life or work domain.	Yes
H2:	An employee's location while using the device (i.e., using the device at home vs. using the device in the workplace) impacts the employee's perceptions of whether they are in the life or work domain.	Yes
H3:	Time of device usage by the employee (i.e., using the device outside normal working hours vs. using the device during normal working hours) impacts employees' perceptions of whether they are in the life or work domain.	Yes
H4:	The type of activity performed by the employee (i.e., personal-related activity vs. work-related activity) impacts employees' perceptions of whether they are in the life or work domain.	Yes
H5a:	Employees' perceptions of the sensitivity of organization-owned data processed on the device (i.e., non-sensitive organization data vs. sensitive organization data) impacts employees' perceptions of whether they are in the life or work domain.	No
H5b:	Employees' perceptions of the sensitivity of personally-owned data processed on the device (i.e., sensitive personal data vs. non-sensitive personal data) impacts employees' perceptions of whether they are in the life or work domain.	No
H6:	The effect of employees' perceived threat severity on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.	Yes
H7:	The effect of employees' perceived threat vulnerability on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.	Yes
H8:	The effect of employees' anticipated rewards on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.	No
H9:	The effect of employees' perceived response efficacy on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.	Yes
H10:	The effect of employees' perceived self-efficacy on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.	Yes
H11:	The effect of employees' response cost on their intention to comply with the information security policy differs depending on their perceptions of whether they are in the work or in the life domain resulting from BYOD.	Yes

CHAPTER SIX: DISCUSSION & CONCLUSION

The previous chapters presented the research models, the approach to testing these models, and the results of these tests. This chapter will discuss these results and present the findings of this thesis. It will also discuss the theoretical and practical implications, describe the research limitations and outline recommendations for future research. The chapter will conclude by presenting the closing statement.

6.1 Summary of the Research

With today's increasing dependency on ICT, information security is becoming one of the most critical areas of concern that organizations need to address to ensure their business sustainability. Adherence to security practices by employees is one of the major challenges faced by organizations as employees have been defined as security's weakest link (e.g., Sasse et al., 2001; Bulgurcu et al., 2010a; Caldwell, 2012). Therefore, there is a great deal of effort by both practitioners and researchers to keep information security policies relevant and to adopt new methods and techniques to ensure employees' behaviors are compliant with these policies.

One of the new strategies introduced by ICT in organizations today is the concept and practice of bring your own device (BYOD). In this strategy, organizations allow their employees to use their own devices to do work-related activities from any place at any time. In 2020, this has become more widespread due to the COVID-19 pandemic, where work from home became the de facto way of operation, resulting in many employees using their own devices to work from home. Although BYOD promises organizations benefits such as employee satisfaction, usability, mobility, efficiency, productivity, and lower operational costs, it also comes with many challenges, information security being a key one.

Traditionally, information security policies and strategies have been designed to regulate employees' behaviors to ensure compliance with information security policies. However, such policies are usually designed to regulate employees' behaviors in the work domain only and assume a clear boundary between the work and life domains. BYOD, though, blurs the boundaries between the two, increasing the complexity of usage scenarios, and creating ambiguity in work ethics which leads to employees' developing their interpretation of BYOD concerning the work-life domain and adopting their own rules and norms.

The information security literature has employed several theories to better understand employee behaviors; however, most of these studies focused mainly on organizational settings, with only a few examining information security outside of the work domain and just two the phenomenon of contextual aspects of BYOD: not all of the unique factors related to BYOD have been fully investigated and discussed. Moreover, no study had put forward a comprehensive framework that captured the complexity of BYOD and defined related contextual factors that influence employees' interpretation of BYOD as a life domain or work domain, and nor had the implications of these factors for information security-related behaviors been identified. Hence, this thesis asks, "How do bring your own device contextual factors affect employees' compliance with information security policies?" In order to answer this question, four objectives were set by this study: 1) to develop a comprehensive conceptualization of BYOD contextual factors, 2) to empirically validate the effect of the BYOD contextual factors on employees' interpretation of the work-life domain perspective, 3) to examine the impact of employees' interpretation of BYOD on compliance with the information security policy, and 4) to empirically validate the research model.

To answer the above research questions, this thesis draws on literature from both information security, to extend border theory, and from work-life domain management literature with two additional factors, i.e., device ownership and data sensitivity, as BYOD contextual factors. Then, the validity of extended BYOD contextual factors was empirically examined. To investigate the third and fourth questions, PMT, one of the most widely-used theories to explain compliance with information security policy, was used as a base model to develop and empirically examine the impact of employees' perceptions of being in the life domain, work domain, or the gray area.

To test the research models, a scenario-based survey was designed for data collection. The survey was published through an on-line platform to recruit participants and an incentive was offered as a reward for completing the survey. Only participants with a high rating based on their previous survey participation in other studies were allowed to take the survey. Each participant was requested to read a randomly presented scenario and then complete the survey. A total of 3035 usable responses were captured, and multiple regression analyses were used to test the two models of this study.

The empirical results show that only four factors can be considered as border-defining factors. The first is device ownership, which captures whether employees are using devices provided

by their organization or their personally-owned devices. The second factor, employees' location, is related to whether the employees are on or outside work premises. The third BYOD contextual factor is the time of activity, reflecting whether the activity was performed during working or non-working hours. The fourth is the activity type: work-related or personal-related behavior. A fifth factor, data sensitivity, was not found to be significant. Therefore, BYOD contextual factors were shown to affect employees' perception of work-life domain. Activity type was the most influential factor in employees determining whether they are in the life domain, work domain, or are unable to differentiate between the two, an area this study referred to as the gray area. This was followed by employees' location, time of activity, and finally device ownership, in terms of their effect on employees' perception of work-life domain.

When it comes to the impact of work-life domain interpretation of BYOD, the results showed that most PMT variables changed their effect on employees' intention to comply with the information security policy based on whether they were in the life domain, the work domain, or the gray area. In particular, when a BYOD usage scenario is considered as a work domain, the perceived threat severity and perceived threat vulnerability factors were found to be significant in affecting employees' intention to comply with information security policy. When BYOD usage scenario is interpreted as a life domain, response efficacy and self-efficacy factors remain significant but with a much stronger effect size while perceived threat severity and perceived threat vulnerability factors lose their significance. For scenarios considered as grey, all PMT factors were significant. Only perceived response efficacy had a consistent effect on employees' intention to comply with information security policy regardless of the employees' perception of work-life domain.

6.2 Discussion of Findings

This section will provide a discussion of the findings of this thesis, mainly focusing on the two proposed models. It will start by discussing the first model proposed in this thesis, highlighting how BYOD contextual factors affect the perception of employees when it comes to being in the work domain or in the life domain. After that, the discussion will focus on the second model in order to show how employees' perceptions of being in the work domain or in the life domain affect their information security compliance behaviors.

6.2.1 Impact of BYOD Contextual Factors on Employees' Perception of Work-Life Domain

This thesis aimed to define BYOD contextual factors and examine their effect on employees' perception of being in the life domain, work domain, or being unable to define which they were in. Accordingly, BYOD contextual factors were developed based on border theory (Clark, 2000). Border theory defines three borders: physical, temporal, and psychological. The first two are very clear, and their adoption in different studies is a straightforward activity. Most prior studies have focused on social and behavioral aspects when defining the psychological border (e.g., Ashforth et al., 2000; Olson-Buchanan and Boswell, 2006; Park and Jex, 2011; Fonner and Stache, 2012); however, in this thesis, two additional borders relevant to the context of BYOD were defined and used as psychological boundaries—device ownership and data sensitivity.

The result of the study showed device ownership to have a significant impact on employees' perception of whether they were in the life or work domain. This is the result of employees adopting different strategies to manage their integration or segmentation of the work-life domain, in particular when it comes to crossing a psychological boundary (Clark, 2000; Dén-Nagy, 2014). Some employees infer that they are in a work domain due to them using company-owned devices while others infer being in a life domain because they are using their personally-owned devices; yet others found themselves unable to make sense of the domain they are in, the so-called 'gray area'.

Previous studies had showed that employees' usage of company-owned smartphones had a negative effect on the life domain (Cavazotte et al., 2014; Duxbury et al., 2014). This thesis confirms their findings: the results showed a positive correlation between employees using their company-owned devices and their perception of being in the work domain. This thesis also examined the effect of using personally-owned devices and showed that there is a positive correlation between employees using their own devices and their perception of being in the life domain.

Examining these results through the lens of border theory provides a new interpretation of how device ownership can affect the work and the life domains. Border theory states that people are border-crossers and that they can either be segmentors or integrators (Clark, 2000). Their success at crossing depends on the strategies [they] adopt, the strength and flexibility of each border, and the permeations that affect the people (Clark, 2000). As this thesis showed that device ownership affects employees' perception of being in the work domain or life domain,

then, as a psychological border, device ownership is considered a strong border that affects employees' border crossing. As stated in border theory, allowing individuals to work from any location and at any time means a high degree of flexibility for physical and temporal borders. This had become the case with many work arrangements due to increased demands from employers and, more recently, has become even more the norm during the 2020 COVID-19 pandemic. In such a flexible work arrangement, both the temporal and physical borders might prove insufficient as a means for employees to segment their work and life domains and might even contribute to their blending. Adding device ownership as an additional border can help researchers to examine work-life studies from a fresh perspective.

Further, the usage of company-owned devices can trigger a spillover from the work domain to the life domain, and BYOD can trigger a spillover from life domain into the work domain. This spillover affects how employees segment the work domain from the life domain when using their own devices in both the work environment or the life environment. The spillover, as indicated by prior studies, can have a negative effect on work-life balance (Chesley, 2005). Therefore, organizations should be aware of such effects and ensure that their employees are educated and trained to address such issues in order to improve their wellbeing.

This is one of the key contextual factors that differentiates BYOD from normal technology usage by employees in organizations. In a normal organizational setting, to carry out work activities, employees use technologies provided by the organization, while in organizations adopting BYOD strategies, employees can use their personally-owned devices. Therefore, this result shows that BYOD impacts employees, specifically when it comes to how they interpret the work-life domain and their ability to segment and integrate these domains.

This thesis also suggested another new border—data sensitivity—but did not find any significant effect for it. This study posited that based on the sensitivity of the data being processed by employees, i.e., whether this information is owned by the organization or personal, their perception of work-life domain will be affected. However, the result of the analysis did not support this, as both Hypotheses 5a and 5b were found to be not supported. Data sensitivity has been hypothesized as triggering employees to cross a psychological ownership boundary (Clark, 2000; Anderson and Agarwal, 2010). However, the result suggests that whether the employees perceive the data being processed as sensitive or not does not affect whether they perceive themselves as being in the life or work domain. One aspect that might have led this result to be insignificant is employees having both sensitive personal data and

sensitive company data on the same device, making it difficult to assess the effect of each data sensitivity.

The other factors adopted from border theory to develop BYOD contextual factors (employees' location, type of activity, and time of activity) were also supported by the results of this thesis. This means that employees' location—being on the work premises (such as in the office) or being away from work premises (such as being at home)—will affect their perception of being in the work or life domain. This accords with previous findings that employees have to manage the spatial boundary (Ashforth et al., 2000; Clark, 2000; Duxbury et al., 2014) in order to integrate or segment the work and life domains. Based on how individuals manage this boundary, their making sense of being in a life domain or work domain may differ and affect which of the two domains (or the gray area) that they perceive themselves to be in.

Similarly, the time of using the device was found to have a significant impact on employees' perception of the work-life domain. Based on the time employees use the device, their interpretation of the work-life domain will change. This accords with the literature where the temporal boundary was identified as a key boundary that individuals need to cross to make sense of being in a life domain or a work domain (Ashforth et al., 2000; Clark, 2000). The impact of time has increased nowadays with new emerging technologies that are highly dependent on the internet. Employees are more flexible about doing personal activities during working hours and work activities after working hours. In addition, unless employees adopt a specific strategy to segregate the two domains (e.g., such as turning off their mobile phone after working hours), they will be available almost 24/7 due to such technologies. This availability will also be expected by the organizations after working hours and at the weekends (Dén-Nagy, 2014; Garba et al., 2015) and this expectation can affect employees' ability to manage their transition from one domain to another.

The type of activities being performed by the employees was found to significantly impact their perceptions of the work-life domain, supporting Hypothesis 4. This accords with Park et al.'s (2011) claim that managing the segmentation and integration of the work and life domains requires a behavioral boundary. With BYOD, employees can perform both personal and work-related activities at any time. Accordingly, employees may cross the behavioral boundary to perceive being in a work domain or being in a life domain. They may respond to a personal email, followed by responding to a work email; they may read a work-related document, then share a post on social media. All of this can have a varying impact on how employees make

sense of where they fall in terms of work-life domain at the moment of performing the activities. For some, their segmentation strategies may be more stringent, and they may delineate between the two domains; others may totally integrate the two domains, while some may fall into a gray area.

When it comes to the control variables, marital status, education, and scenario realism were found to have a significant effect on employees' perception of the work-life domain, the strongest effect coming from marital status. Married employees were reluctant to perceive themselves to be in the work domain, and more eager to interpret themselves as being in the life domain. It might be that due to the employees' commitment to their family, they aim to segregate the two domains more. Nevertheless, in one study, married employees with more children were found to be more worried about work during non-working hours than married employees with fewer children; the study also concluded that married employees would have more difficulty managing work-life balance than those that are unmarried (Vasumathi et al., 2015). This might be the reason why the effect of marital status was negative. However, further study may be required to investigate this and shed more light on the effect of marital status.

The results show that level of education also had a negative effect on employees' perception of work-life domain, meaning that the higher their education level is, the more they will be inclined to interpret themselves being in the life domain, while less educated employees will lean more toward the work domain. More studies may also be required on this to determine the reason for this result. It may be due to more educated employees having more job security, which is why their work commitment is less than those with less education that feel less secure about their job and think about it after working most of the time. Another reason may be that the more educated individual will have better time management skills and more focused mental capabilities to segregate the two domains in comparison to those that have less education. Other explanations might exist; however, more qualitative studies would be better able to explore this domain.

Listing the BYOD contextual factors in order of effect size, type of activity comes first followed by employees' location, time of activity and finally device ownership. As a result, employees' perception of work-life domain will be mostly influenced by the type of activities they are performing—meaning in many cases, even if the employees are in the office (i.e., the location most associated with the work domain) during working hours (i.e., the time of activity mostly associated with the work domain), and using work-provided devices (i.e., device

ownership mostly associated with the work domain), if they are performing personal activities such as calling their spouse or posting on social media (i.e., the type of activity mostly associated with the life domain), employees may associate themselves with being in the personal domain. However, this might not be the case for most employees, as each may be more influenced by one of the other factors. Moreover, the aspect of each factor may also have a huge impact. For example, a personal activity such as calling a spouse may not have the same effect on the person's perception of work-life domain as posting on social media or even reading a comic book. This is an area that may merit further investigation by future research.

In addition, as we do not live in a linear world, BYOD contextual factors coexist, and different mixes of aspects from each BYOD contextual factor will come together. For example, an employee might be in the office, after working hours, doing work-related activities using his own device. These mixes of aspects from each BYOD contextual factor will have different effects for different employees. Some may have a stronger ability to segregate their work and life domains, while others may completely blend the two and fall into a gray area.

Based on the above results, the proposed BYOD contextual factors were revised by removing the data sensitivity. The four main revised BYOD contextual factors that this study proposed in order to address the first research question are shown in Table 30. Based on the work-life balance literature (Ashforth et al., 2000; Clark, 2000; Olson-Buchanan and Boswell, 2006; Park and Jex, 2011; Fonner and Stache, 2012) and the result of the analysis for Model 1, we find that employees use psychological, physical, temporal, and behavioral boundaries. Device ownership is a psychological boundary that employees need to manage to determine their presence in one or other of the work-life domains; thus, device ownership was defined as a key BYOD contextual factor. Whether the device is owned by the organization or by the employee will affect how the employees make sense of their work-life domain.

Similarly, an employee's location is a physical boundary that influences their perception of work-life domain and, therefore, was stated as a second BYOD contextual factor. Being on or outside of the work premises is another determinant for employees' ability to define and manage their work-life domain transition. The third BYOD contextual factor is the time of activity, which is a temporal boundary between the life domain and the work domain. Performing activities on the device during working or non-working hours is another aspect that influences employees' work-life domain perceptions. The final BYOD contextual factor is related to the behavioral boundary, which is the activity type performed by the employee.

Doing personal activities will have a different influence on employees' work-life domain perceptions than doing work-related activities.

Further, the results also showed that each BYOD contextual factor has an aspect that can influence employees' perception of life or work domains. For example, looking at activity type as a BYOD contextual factor, individuals performing work-related activities such as writing a report or undergoing a job performance review will trigger employees toward associating themselves as being in the work domain while employees performing personal activities such as reading the news or browsing social media will lean toward associating themselves with the life domain.

This summarizes the four BYOD contextual factors that are posited by this study, namely 1) device ownership, 2) employees' location, 3) time of activity, and 4) activity type. Each contextual factor has aspects that influence employees' perception of themselves as being in either the life or work domain.

TABLE 30: REVISED BYOD CONTEXTUAL FACTORS

BYOD Contextual Factors	Life-Associated Aspects of BYOD Contextual Factors	Work-Associated Aspects of BYOD Contextual Factors
Device Ownership	Employees use their personal devices (e.g., smartphones, laptops, tablets) rather than devices owned by their organization.	Employees use the organization's devices (e.g., workstations, smartphones, laptops, tablets).
Employees' Location	Employees use the devices in a non-work environment (e.g., home, coffee shops, hotels).	Employees use the devices on the organization's premises (e.g., office, meeting rooms, other branches).
Time of Activity	Employees use the devices during non-working hours.	Employees use the devices during working hours.
Activity Type	Employees use the devices to work on personal tasks (e.g., social media, personal emails, reading news, browsing the internet).	Employees use the devices to perform work-related tasks (e.g., developing reports, processing transactions, responding to work emails).

This result is highly relevant to the context of the 2020 COVID-19 pandemic. Where feasible, almost the whole world has adopted work from home, and BYOD contextual factors provide a lens through which to view this phenomenon. More specifically, in this phenomenon, employees are working (i.e., type of activity) from home (i.e., employees' location), during or after working hours (i.e., time of activity), and using their personal or work devices (i.e., device ownership).

Organizations that are aiming to ensure their employees' wellbeing with a balanced work-life balance and thus gain more productive and loyal employees, can benefit from the above results. ICT has been shown in prior studies to be a tool that can both affect the work-life balance negatively and also be used to manage the two worlds (Golden and Geisler, 2007; Hubers et al., 2011; Sayah, 2013). These organizations can implement awareness strategies to assist their employees to use their devices as a way to segment the domains and ensure that a balance between work and life is reached.

6.2.2 Compliance with Information Security Behavior from the Work-Life Domain Perspective

The second objective of this thesis is to show whether employees' perception of work-life domains affects their compliance behaviors in regard to information security policies. Model 2 adopted the variables of protection motivation theory to test their relationships with employees' intentions to comply with their organization's information security policy. This relationship was tested in three different groups: those individuals that perceived themselves to be in the life domain; those who perceived themselves to be in the work domain; and, those that were not able to define which domain they are in and found themselves in the gray area between the two. The variables from protection motivation theory were shown to have a different effect from one group to another, as shown in Table 31.

TABLE 31: MODEL 2 – RESULTS SUMMARY

	Life	Gray	Work
Perceived Threat Severity (PTS)	Not Supported	Supported	Supported
Perceived Threat Vulnerability (PTV)	Not Supported	Supported	Supported
Reward (RWD)	Not Supported	Supported (Negative Direction)	Not Supported
Response Efficacy (RE)	Supported	Supported	Supported
Self-Efficacy (SE)	Supported	Supported (Negative Direction)	Supported
Response Cost (RC)	Not Supported	Supported	Not Supported

For example, the relationship between perceived threat severity and employees' intention to comply with the information security policy changed based on their perception of which domain they were in. In the life domain, the perceived threat severity was shown not to have any significant effect on employees' intention to comply with information security policy; in the work domain, however, it had a significant effect. This result supports the argument of this thesis that employees' cognitive processes to formulate their intention to (non-)comply with information security policy differs and is affected differently in the work domain in comparison to the life domain. For example, perceived threat severity had a significant effect on compliance with information security policy when employees use organizational devices (Vance et al., 2012; Pahnila et al., 2013; Siponen et al., 2014; Johnston et al., 2015), but not when they use their own devices (Crossler et al., 2014; Dang and Pittayachawan, 2015). However, each of these studies focused on only one aspect of the device ownership, whether the device was owned by the organization or by the employees, and did not compare these two aspects of device ownership as suggested here. Furthermore, this thesis used border theory to show how device ownership affects the perceptions of being in the work-life domain, and subsequently, how this perception affected employees' information security policy. This provides a way to interpret the changes in the effect for different variables in a different context that prior studies did not discuss.

An interesting and unexpected finding from the results is that out of all the variables from protection motivation theory, only one factor remained constant in the three groups. While perceived threat severity, perceived threat vulnerability, rewards, perceived response efficacy,

perceived self-efficacy, and response cost all had a different effect on employees' intention to comply with information security policy based on their perception of work-life domain, the relationship between employees' perceived response efficacy and their intention to comply with the information security policy was found to be significant regardless of employees' perceptions of the work-life domain. This result is consistent with prior research where the location of usage was included in the research model (e.g., Dang and Pittayachawan, 2015). In line with prior research on information security (e.g., Herath and Rao, 2009a; Johnston and Warkentin, 2010; Ifinedo, 2012; Siponen et al., 2014; Sommestad et al., 2015; Hanus and Wu, 2016) this result shows that the impact of perceived response efficacy could be generalized to both the life and work domains.

The results above are related to PMT variables; however, similar results might occur if different theories were used. Some of the common theories in the information security behavioral literature, such as the theory of reasoned action and deterrence theory, are good candidates for future studies to use to test the effect of employees' perception of work-life domain on their intention to comply with information security policy. Such studies could further support the results of this study and shed light on those factors that remain constant regardless of the domain employees perceive themselves to be in. In addition to investigating employees' intention to comply with information security policy, future research can investigate the effect of employees' perception of work-life domain on other types of employee behavior and perceptions such as performance, job satisfaction and quality of life. With the widespread adoption of ICT, employees' perception of work-life domain is a critical factor in their day-to-day operations; therefore, such studies will provide more insight into how it affects them and offer recommendations that contribute positively to this phenomena, both for employees and organizations.

Practically, the results provide evidence of the importance of employees' perception of the work-life domain as it affects how they perform their work and comply with their organizations' information security policy. Organizations will need to ensure that their information security policies address the usage of personal devices and the different BYOD contextual factors. Further, organizations' communication strategies should focus more on those factors that remain constant regardless of the employees' perception of work-life domain as these will have a stronger effect on their behavior.

6.3 Theoretical Implications

This thesis offers several theoretical contributions. First, it has developed a comprehensive view of BYOD contextual factors that offers a fresh perspective and an opportunity to re-examine the usefulness of existing theories in explaining BYOD-related employee behaviors. The empirical validation of the BYOD contextual factors in employees' perception of the work-life domain refines and updates the existing framework by identifying four important factors and suggesting the existence of the gray area where the interpretation might be ambiguous. This contributes to existing border theory by enriching the border factors and enhancing its ability to accommodate new technological developments. This extension also shows the complexity of separating work from life, similar to prior studies (e.g., Chesley, 2005; Leung, 2011). With the increasing penetration of technologies into people's daily lives, the work-life boundary will be further fragmented and blurred, and hence the assumption that people can clearly distinguish between the work and life domains needs to be challenged and investigated in future research. As indicated in this thesis, it was difficult to classify some scenarios as clearly one or the other. This reflects the ongoing challenges of making sense of new technologies and coping with the gaps between increasing individual computing power and now outdated organizational policies (e.g., Garba et al., 2015; Palanisamy et al., 2020a; Palanisamy et al., 2020b).

This thesis further shows how the work-life domain perception induced by BYOD could alter the explanatory power and findings of existing theories in information security. While the majority of existing literature is on information security-related behavior in an organizational context, using organizational devices while being in the work-domain, the results of this thesis suggest that information security research also needs to accommodate and investigate non-work domains (Li and Siponen, 2011). In this study, PMT was selected and tested when employees perceived themselves to be in life or work domains, and in the gray area. The results reveal that, apart from response efficacy, the PMT variables do not have consistent explanatory power across three groups, confirming our hypotheses. In other words, since individuals follow different rules and norms in different domains, their interpretation of technologies in use would imply different sets of meta-cognition. Thus, the work-life domain is a valid theoretical boundary that may limit the generalization of existing information security research, and future research should take this into account.

6.4 Practical Implications and Recommendations

With the increased adoption of ICT by organizations to run their day-to-day operations and by employees as a necessity in their daily activities, the perception of work-life domain has become a critical area that needs to be taken into consideration. Further, evidence shows that dependency on ICT will only increase in the future. The introduction of new devices with more capabilities and factors (such as connectivity via 5G) only makes it even more important that both practitioners and academics better understand the effect of BYOD contextual factors. Therefore, more research is required to provide more insight into this phenomena. The results of this study play a role in that by guiding practitioners in the field of information security, in general, and (more specifically) in BYOD implementation.

Practically, the results provide evidence of the importance of employees' perception of work-life domain in its effect on how they perform their work and comply with their organizations' information security policy. Organizations will need to ensure that their information security policies address the usage of personal devices and the different BYOD contextual factors. Further, organizations need to be informed about home-user studies and information security behaviors in order to reflect their findings in their information security policies and ensure that they remain relevant.

In addition, the results of this study support organizations in designing their security behavioral change programs. Such intervention programs—whether delivered in the form of training, awareness programs, or introductions to new policies—can be tailored to capture the unique contextual factors of BYOD. Further, response efficacy was found to remain constantly relevant in influencing employees' intention to comply with information security policy. This will help practitioners to design intervention messages in their information security awareness, communications, and training to target this specific factor to promote compliant behaviors. Other PMT variables can be included based on the particular objectives of these intervention programs, the work-life domain they are targeting, and the organization's appetite for risk. Therefore, a better understanding of the impacts of the different factors will contribute to the effectiveness of these programs in achieving their objectives. For instance, the consistent result of the impact of response efficacy across the work-life domains suggests that this should be a key focus in developing communication strategies to influence employees' compliance with information security policies. Such communication strategies can include key messages demonstrating the effectiveness of various actions in protecting the devices they are using.

Future research could focus on defining which factors that emerge from testing different variables in different contexts that can be proved to be more effective in changing employees' behavior.

The results of this study are even more relevant today with the 2020 global adoption of work from home (WFH) due to COVID-19. The majority of the population in the world has been working from home, many using their own devices. Extant information security policies were not written to address this aspect, and many organizations have begun to share awareness communications to ensure that their employees adopt information security behaviors that will assure the protection of organizations' assets. It is expected that work from home will remain as the approach adopted by many organizations in post-COVID-19 times and this concept might even be expanded to be replaced with work from anywhere (WFX). Such a change would certainly bring new challenges and security threats. It is highly unlikely that our pre-pandemic normal day-to-day life will survive; it has already been replaced with different ways of working, interacting, and engaging, what is already being referred to by many as the 'new normal' (Papageorghiou, 2020). This thesis, based on the BYOD contextual factor it posits, provides a starting point for future studies to examine different work-related behaviors from a new perspective to support these practices and the adoption of new technologies in the future. More specifically, this thesis can guide organizations in the new normal to address the new security challenges they will face as a result of new business models and technology adoptions.

6.5 Limitations and Future Research

There are a few limitations that may prevent generalization of the results of this thesis, which also imply interesting future research. First, in this study, the focus was on limited aspects of each BYOD contextual factor. For example, for employees' location, home and work were used. However, other locations such as a coffee shop or a mall may have a different effect and may contribute to a different perception of employees' work-life domain. Similarly, with device ownership, the device might be borrowed from a friend or a co-worker instead of being a personally-owned or company-provided device. In addition, this thesis only used laptops as a testing device. Given the diversity in computing devices, such as mobile devices, it might be worthwhile to study the usage of different technologies because each technology will bring its own unique characteristics. For example, an employee might feel more intimate with the usage of a smartphone that s/he carries all the time and has mixed usage of personal and work activities rather than with a laptop. Therefore, such aspects might provide another dimension

that may have a significant influence on employees' perception of work-life domain. In addition, future studies could further investigate the different aspects of each BYOD contextual factor.

Second, the sample in this thesis consisted of full-time employees. The type of employment may contribute to further complexity, e.g., freelancers or contract-based employees. One possible impact might be the different weight of BYOD contextual factors in defining work-life domains. For those organizations with more open and flexible human resource management, it would be worthwhile replicating this research to investigate how employees with different employment relationships may have different interpretations of BYOD.

It would also be interesting to study factors other than BYOD contextual factors that influence employees' perception of work-life domain. The results showed that BYOD contextual factors were responsible for only 33.1% of the changes in employees' perception of the work-life domain. Therefore, 66.9% remains unexplained. Accordingly, this study urges future researchers to investigate further the other factors that play a role in formulating employees' perception of the work-life domain.

Fourth, in testing the impact of work-life domain perception induced by BYOD, this thesis chose PMT as an example due to its popularity in information security research. Future studies could also test the effect that employees' perception of work-life domain has on information security behavior based on other theories. This study focused only on PMT; however, other theories have been used in the information security literature to understand the predictors of information security-related behaviors and the factors influencing these behaviors, for example, the theory of reasoned action or deterrence theory. This was also suggested by other studies (Palanisamy et al., 2020a). These studies could further support the results of this study. In addition, they could define additional factors that remain constant regardless of the domain employees perceive themselves in, such as perceived response efficacy. These constant factors could be a key area for organizations to use in their communication strategies to influence employees' behavior toward complying with information security policy.

An interesting area to be further investigated is the effect of the gray area on employees' intention to comply with information security policy. The results showed how the effect of the factors influencing employees' intention to comply with information security policy changed from one domain to another. As the majority of studies available focus exclusively on the home

or work setting, further studies on the gray area will provide better insight into how this area affects employees' information security behavior.

Future studies could also examine the effect of employees' perception of work-life domain on other behaviors. This study only focused on the effect of employees' perception of work-life domain on their intention to comply with information security behavior. However, a similar effect might appear for other behaviors, for example relating to knowledge-sharing, absenteeism, turnover, or job performance. With the high dependency of organizations on ICT, and as the effect of BYOD contextual factors can be introduced by different devices regardless of their ownership, where in some cases, employees will build a sense of ownership of the device even if it is provided and owned by the organization, it would be interesting to determine how BYOD contextual factors can affect different behaviors.

6.6 Closing Statement

In conclusion, the field of information security is growing day by day. With this growth, one of the most challenging factors in the information security field is human behaviors. Many previous studies used several theories in order to understand employees' behaviors in regard to complying with information security policy. This study contributed to this field of research by defining a new phenomenon brought about by a new trend of employees bringing their own devices to use in work-related activities. The study provides evidence of the effect that BYOD contextual factors have on employees' perception of the work-life domains. In addition, it showed the effect of this perception on employees' intentions to comply with information security policy. This opens the path for many future studies to examine BYOD contextual factors further and provide more recommendations to improve information security practices.

REFERENCES

AHMAD, Z., ONG, T. S., LIEW, T. H. & NORHASHIM, M. 2019. Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information and Computer Security,* 27**,** 165-188.

AJZEN, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes,* 50**,** 179-211.

AJZEN, I. 2012. Martin Fishbein's Legacy: The Reasoned Action Approach. *The Annals of the American Academy of Political and Social Science,* 640**,** 11-27.

AKERS, R. L. 1990. Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken. *Journal of Criminal Law and Criminology,* 81**,** 653-676.

AL-OMARI, A., DEOKAR, A., EL-GAYAR, O., WALTERS, J. & ALEASSA, H. Information Security Policy Compliance: An Empirical Study of Ethical Ideology. 2013 46th Hawaii International Conference on System Sciences, 7-10 January 2013 Hawaii. Hawaii: IEEE Computer Society, 3018-3027.

ALASKAR, M., VODANOVICH, S. & SHEN, K. N. Evolvement of Information Security Research on Employees' Behavior: A Systematic Review and Future Direction. 2015 48th Hawaii International Conference on System Sciences, 2015. IEEE, 4241-4250.

ALONSO, O. & BAEZA-YATES, R. Design and implementation of relevance assessments using crowdsourcing. European Conference on Information Retrieval, 2011. Springer, 153-164.

ALSHARE, K. A., LANE, P. L. & LANE, M. R. 2018. Information security policy compliance: A higher education case study. *Information and Computer Security,* 26**,** 91-108.

AMANKWA, E., LOOCK, M. & KRITZINGER, E. 2018. Establishing information security policy compliance culture in organizations. *Information and Computer Security,* 26**,** 420-436.

ANDERSON, C. L. & AGARWAL, R. 2010. Practicing Safe Computing: A Multimethod Empirical Examination Of Home Computer User Security Behavioral Intentions. *MIS Quarterly,* 34**,** 613-A15.

ARMITAGE, C. J. & CONNER, M. 2000. Social cognition models and health behaviour: A structured review. *Psychology & Health,* 15**,** 173-189.

ARMITAGE, C. J. & CONNER, M. 2001. Efficacy of the theory of planned behaviour: A meta-analytic review. *The British Journal of Social Psychology,* 40**,** 471.

ASHFORTH, B. E., KREINER, G. E. & FUGATE, M. 2000. All in a day's work: Boundaries and micro role transitions. *Academy of Management Review,* 25**,** 472-491.

AURIGEMMA, S. & MATTSON, T. 2017. Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security,* 25**,** 421-436.

BANDURA, A. 1977. Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review,* 84**,** 191.

BANDURA, A. 1986. *Social Foundations of Thought and Action: A Social Cognitive Theory,* Englewood Cliffs, NJ, US, Prentice-Hall, Inc.

BARGER, P., BEHREND, T. S., SHAREK, D. J. & SINAR, E. F. 2011. IO and the crowd: Frequently asked questions about using Mechanical Turk for research. *TIP,* 49**,** 11-18.

BARLOW, J. B., WARKENTIN, M., ORMOND, D. & DENNIS, A. R. 2013. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security,* 39:B**,** 145-159.

BECCARIA, C. 2013. *On Crimes and Punishment,* Lexington, Kentucky, USA, Branden Books.

BECKER, G. S. 1968. Crime and punishment: An economic approach. *The Economic Dimensions of Crime.* London: Palgrave Macmillan.

BECKER, M. H. 1974. The Health Belief Model and Personal Health Behavior. *Health Education Monographs,* 2**,** 324- 508.

BEHREND, T. S., SHAREK, D. J., MEADE, A. W. & WIEBE, E. N. 2011. The viability of crowdsourcing for survey research. *Behavior Research Methods,* 43**,** 800.

BÉLANGER, F., COLLIGNON, S., ENGET, K. & NEGANGARD, E. 2017. Determinants of early conformance with information security policies. *Information & Management,* 54**,** 887-901.

BERKOWSKY, R. W. 2013. When you just cannot get away. *Information, Communication & Society,* 16**,** 519-541.

BERNARDESCHI, C., DE FRANCESCO, N. & LETTIERI, G. 2002. An abstract semantics tool for secure information flow of stack-based assembly programs. *Microprocessors and Microsystems,* 26**,** 391-398.

BISSELL, K., LASALLE, R. M. & CIN, P. D. 2019. Cost of Cybercrime. Accenture

BISSELL, K., LASALLE, R. M. & CIN, P. D. 2020. Innovate for Cyber Resilience. Accenture.
BOSS, S., GALLETTA, D., LOWRY, P. B., MOODY, G. D. & POLAK, P. 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly,* 39**,** 837-864.
BOSS, S. R., KIRSCH, L. J., ANGERMEIER, I., SHINGLER, R. A. & BOSS, R. W. 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems,* 18**,** 151-164.
BOUDREAU, M.-C., GEFEN, D. & STRAUB, D. W. 2001. Validation in Information Systems Research: A State-of-the-Art Assessment. *MIS Quarterly,* 25**,** 1-16.
BRADLEY, J., LOUCKS, J., MACAULAY, J., MEDCALF, R. & BUCKALEW, L. 2012. BYOD: A global perspective, harnessing employee-led innovation, Cisco IBSG Horizons.
BRAGGER, J. D., RODRIGUEZ-SREDNICKI, O., KUTCHER, E. J., INDOVINO, L. & ROSNER, E. 2005. Work-family conflict, work-family culture, and organizational citizenship behavior among teachers. *Journal of Business and Psychology,* 20**,** 303-324.
BRUBAKER, R. G. & FOWLER, C. 1990. Encouraging College Males to Perform Testicular Self-Examination: Evaluation of a Persuasive Message Based on the Revised Theory of Reasoned Action. *Journal of Applied Social Psychology,* 20**,** 1411-1422.
BUHRMESTER, M., KWANG, T. & GOSLING, S. D. 2011. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science,* 6**,** 3-5.
BULGURCU, B., CAVUSOGLU, H. & BENBASAT, I. Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. 2009 International Conference on Computational Science and Engineering, 2009. IEEE, 476-481.
BULGURCU, B., CAVUSOGLU, H. & BENBASAT, I. 2010a. Information Security Policy Compliance: An Empirical Study Of Rationality Based Beliefs And Information Security Awareness. *MIS Quarterly,* 34**,** 523-527.
BULGURCU, B., CAVUSOGLU, H. & BENBASAT, I. Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: An empirical investigation. 2010 43rd Hawaii International Conference on System Sciences, 2010b. IEEE, 1-7.
BURMEISTER, C. P., MOSKALIUK, J. & CRESS, U. 2018. Ubiquitous working: do work versus non-work environments affect decision-making and concentration? *Frontiers in Psychology,* 9**,** 310.
BURNS, A., POSEY, C., ROBERTS, T. L. & LOWRY, P. B. 2017. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior,* 68**,** 190-209.
CALDWELL, T. 2012. Training - the weakest link. *Computer Fraud & Security,* 2012**,** 8.
CAVAZOTTE, F., HELOISA LEMOS, A. & VILLADSEN, K. 2014. Corporate smart phones: Professionals' conscious engagement in escalating work connectivity. *New Technology, Work and Employment,* 29**,** 72-87.
CHAN, M., WOON, I. & KANKANHALLI, A. 2005. Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy & Security,* 1**,** 18-41.
CHEN, X., WU, D., CHEN, L. & TENG, J. K. L. 2018. Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management,* 55**,** 1049-1060.
CHEN, Y. K. W. K.-W. 2012. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems,* 29**,** 157-188.
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.
CHENG, W. & SHI-BO, W. 2014. User behavior research of information security technology based on TAM. *International Journal of Security and Its Applications,* 8**,** 203-210.
CHESLEY, N. 2005. Blurring boundaries? Linking technology use, spillover, individual distress, and family satisfaction. *Journal of Marriage and Family,* 67**,** 1237-1248.
CHRISTENSEN, T. H. 2009. 'Connected presence'in distributed family life. *New Media & Society,* 11**,** 433-451.

CHUA, H. N., WONG, S. F., LOW, Y. C. & CHANG, Y. 2018. Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics,* 35**,** 1770-1780.
CLARK, S. C. 2000. Work/family border theory: A new theory of work/family balance. *Human Relations,* 53**,** 747-770.
CLARK, S. C. 2002. Communicating across the work/home border. *Community, Work & Family,* 5**,** 23-48.
COHEN, L., MANION, L. & MORRISON, K. 2013. *Research Methods in Education,* New York, Routledge.
COX, J. 2012. Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior,* 28**,** 1849-1858.
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.
CROTTY, M. 1998. *The Foundations of Social Research: Meaning and Perspective in the Research Process,* London, Sage.
CURRIE, J. & EVELINE, J. 2011. E-technology and work/life balance for academics with young children. *Higher Education,* 62**,** 533-550.
D'ARCY, J. & HERATH, T. 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems,* 20**,** 643-658.
D'ARCY, J., HERATH, T. & SHOSS, M. K. 2014. Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems,* 31**,** 285-318.
D'ARCY, J. & HOVAV, A. 2007. Deterring internal information systems misuse. *Communications of the ACM,* 50**,** 113-117.
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.
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.
DANG, D. P. T. & PITTAYACHAWAN, S. 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security,* 48**,** 281-297.
DANG, D. P. T., PITTAYACHAWAN, S. & NKHOMA, M. Z. Contextual difference and intention to perform information security behaviours against malware in a BYOD environment: A protection motivation theory approach. Australasian Conference on Information Systems (ACIS), 2013. 4-6.
DATALOSSDB-OPEN-SECURITY-FOUNDATION 2013. Data Loss Statistics.
DAVIS, G. 2012. Fortinet global survey reveals 'first generation' BYOD workers pose serious security challenges to corporate IT systems. california: Fortinet.
DÉN ‐ NAGY, I. 2014. A double-edged sword?: A critical evaluation of the mobile phone in creating work ‐ life balance. *New Technology, Work and Employment,* 29**,** 193-211.
DIAZ, I., CHIABURU, D. S., ZIMMERMAN, R. D. & BOSWELL, W. R. 2012. Communication technology: Pros and cons of constant connection to work. *Journal of Vocational Behavior,* 80**,** 500-508.
DISTERER, G. & KLEINER, C. 2013. BYOD bring your own device. *Procedia Technology,* 9**,** 43-53.
DOARGAJUDHUR, M. S. & DELL, P. 2019. Impact of BYOD on organizational commitment: an empirical investigation. *Information Technology & People,* 32**,** 246-268.
DODEL, M. & MESCH, G. 2019. An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security,* 86**,** 75-91.
DONG, X., CLARK, J. A. & JACOB, J. L. 2010. Defending the weakest link: phishing websites detection by analysing user behaviours. *Telecommunication Systems,* 45**,** 215-226.
DUGO, T. 2007. *The insider threat to organizational information security: a structural model and empirical test.* PhD thesis, Auburn University.
DUNKERLEY, K. & TEJAY, G. 2010. Theorizing information security success: Towards secure e-government. *International Journal of Electronic Government Research,* 6**,** 31-41.
DUXBURY, L., HIGGINS, C., SMART, R. & STEVENSON, M. 2014. Mobile Technology and Boundary Permeability. *British Journal of Management,* 25**,** 570-588.

FISHBEIN, M. 2000. The role of theory in HIV prevention. *AIDS Care,* 12**,** 273-278.
FISHBEIN, M. & AJZEN, I. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research,* Mass, Addison-Wesley.
FISHBEIN, M. & AJZEN, I. 2010. *Predicting and changing behavior: The reasoned action approach,* New York, Psychology Press.
FLECK, R., COX, A. L. & ROBISON, R. A. V. 2015. Balancing Boundaries: Using Multiple Devices to Manage Work-Life Balance. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* Seoul, Republic of Korea: ACM.
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.
FONNER, K. L. & STACHE, L. C. 2012. All in a day's work, at home: Teleworkers' management of micro role transitions and the work–home boundary. *New Technology, Work and Employment,* 27**,** 242-257.
FRISSEN, V. A. 2000. ICTs in the rush hour of life. *The Information Society,* 16**,** 65-75.
GARBA, A. B., ARMAREGO, J., MURRAY, D. & KENWORTHY, W. 2015. Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Journal of Information Privacy and Security,* 11**,** 38-54.
GARBA, A. B., ARMAREGO, J., MURRAY, D. & KENWORTHY, W. 2017. A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security,* 25**,** 475-492.
GARRISON, C. P. & NCUBE, M. 2011. A Longitudinal Analysis of Data Breaches. *Information Management & Computer Security,* 19**,** 216-230.
GIBBS, J. P. 1975. *Crime, Punishment, and Deterrence,* New York, Elsevier
GIBBS, J. P. 1979. Assessing the Deterrence Doctrine: A Challenge for the Social and Behavioral Sciences. *American Behavioral Scientist,* 22**,** 653-677.
GOLDEN, A. G. & GEISLER, C. 2007. Work–life boundary management and the personal digital assistant. *Human Relations,* 60**,** 519-551.
GOPAL, R. D. & SANDERS, G. L. 1997. Preventive and Deterrent Controls for Software Piracy. *Journal of Management Information Systems,* 13**,** 29-47.
GUO, K. H. & YUAN, Y. 2012. The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management,* 49**,** 320-326.
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.
HAGEN, J., ALBRECHTSEN, E. & JOHNSEN, S. O. 2011. The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security,* 19**,** 140-154.
HAIR, J. F., BLACK, W. C. & BABIN, B. J. 2010. *Multivariate Data Analysis: A Global Perspective*, Pearson.
HALL, J. H., SARKANI, S. & MAZZUCHI, T. A. 2011. Impacts of organizational capabilities in information security. *Information Management & Computer Security,* 19**,** 155-176.
HAN, J., KIM, Y. J. & KIM, H. 2017. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security,* 66**,** 52-65.
HANKINS, M., FRENCH, D. & HORNE, R. 2000. Statistical guidelines for studies of the theory of reasoned action and the theory of planned behaviour. *Psychology & Health,* 15**,** 151-161.
HANUS, B. & WU, Y. A. 2016. Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. *Information Systems Management,* 33**,** 2-16.
HARRINGTON, S. J. 1996. The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly,* 20**,** 257-278.
HEIJSTRA, T. M. & RAFNSDOTTIR, G. L. 2010. The Internet and academics' workload and work–family balance. *The Internet and Higher Education,* 13**,** 158-163.
HERATH, T. & RAO, H. R. 2009a. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems,* 47**,** 154-165.
HERATH, T. & RAO, H. R. 2009b. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,* 18**,** 106-125.
HIGGINS, G. E., WILSON, A. L. & FELL, B. D. 2005. An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture,* 12**,** 166-184.

HILL, E. J., FERRIS, M. & MÄRTINSON, V. 2003. Does it matter where you work? A comparison of how three work venues (traditional office, virtual office, and home office) influence aspects of work and personal/family life. *Journal of Vocational Behavior,* 63**,** 220-241.
HIRSCHI, T. 1969. *Causes of Delinquency,* Berkeley, University of California Press.
HISLOP, D. & AXTELL, C. 2011. Mobile phones during work and non-work time: A case study of mobile, non-managerial workers. *Information and Organization,* 21**,** 41-56.
HU, Q., DINEV, T., HART, P. & COOKE, D. 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences,* 43**,** 615-660.
HU, Q., XU, Z., DINEV, T. & LING, H. 2011. Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM,* 54**,** 54-60.
HUBERS, C., SCHWANEN, T. & DIJST, M. 2011. Coordinating everyday life in the Netherlands: a holistic quantitative approach to the analysis of ICT‐related and other work‐life balance strategies. *Geografiska Annaler: Series B, Human Geography,* 93**,** 57-80.
HUMAIDI, N. & BALAKRISHNAN, V. 2015. Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology,* 5**,** 311.
HWANG, I. & CHA, O. 2018. Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior,* 81**,** 282-293.
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.
IFINEDO, P. 2014. Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management,* 51**,** 69-79.
IFINEDO, P. 2016. Critical times for organizations: what should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management,* 33**,** 30-41.
INFOSECURITY MAGAZINE. 2012. *Global security spending to hit $86B in 2016* [Online]. Available: http://www.infosecurity-magazine.com/view/28219/global-security-spending-to-hit-86b-in-2016 [Accessed 04 November 2013].
ISO 2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary. *ISO/IEC 27000:2018.* International Organization for Standardization.
ITU 2015. ICT Facts and Figures. Switzerland: International Telecommunication Union.
JALI, M. Z., FURNELL, S. M. & DOWLAND, P. S. 2010. Assessing image-based authentication techniques in a web-based environment. *Information Management & Computer Security,* 18**,** 43-53.
JOHNSTON, A. C. & WARKENTIN, M. 2008. Information privacy compliance in the healthcare industry. *Information Management & Computer Security,* 16**,** 5-19.
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.
JOUINI, M., RABAI, L. B. A. & AISSA, A. B. 2014. Classification of security threats in information systems. *Procedia Computer Science,* 32**,** 489-496.
KAJTAZI, M., CAVUSOGLU, H., BENBASAT, I. & HAFTOR, D. 2018. Escalation of commitment as an antecedent to noncompliance with information security policy. *Information and Computer Security,* 26**,** 171-193.
KANKANHALLI, A., TEO, H.-H., TAN, B. C. Y. & WEI, K.-K. 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management,* 23**,** 139-154.
KONRAD, A. M. & MANGEL, R. 2000. The impact of work‐life programs on firm productivity. *Strategic Management Journal,* 21**,** 1225-1237.
KRUGER, H., DREVIN, L. & STEYN, T. 2010. A vocabulary test to assess information security awareness. *Information Management & Computer Security,* 18**,** 316-316-327.
KUMAR, R. 2019. *Research Methodology: A Step-by-Step Guide for Beginners,* London, SAGE.

LAMBERT, S. J. 2000. Added benefits: The link between work-life benefits and organizational citizenship behavior. *Academy of Management Journal,* 43**,** 801-815.
LANKTON, N. K., STIVASON, C. & GURUNG, A. 2019. Information protection behaviors: morality and organizational criticality. *Information and Computer Security,* 27**,** 468-488.
LEE, S. M., LEE, S.-G. & YOO, S. 2004. An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management,* 41**,** 707-718.
LEE, Y. & LARSEN, K. R. 2009. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems,* 18**,** 177-187.
LEUNG, L. 2011. Effects of ICT connectedness, permeability, flexibility, and negative spillovers on burnout and job and family satisfaction. *Human Technology: An Interdisciplinary Journal on Humans in ICT Environments,* 7**,** 250-267.
LEWIS, S. & COOPER, C. 2005. *Work-Life Integration: Case Studies of Organisational Change*, Wiley Online Library.
LI, H., ZHANG, J. & SARATHY, R. 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems,* 48**,** 635-645.
LI, L., HE, W., XU, L., ASH, I., ANWAR, M. & YUAN, X. 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management,* 45**,** 13-24.
LI, Y. & SIPONEN, M. A Call For Research On Home Users' Information Security Behaviour. PACIS 2011 - 15th Pacific Asia Conference on Information Systems: Quality Research in Pacific, 2011. 112.
LIAO, Q., LUO, X., GURUNG, A. & LI, L. 2009. Workplace Management And Employee Misuse: Does Punishment Matter? *Journal of Computer Information Systems,* 50**,** 49-59.
LIN, T.-C., HSU, M. H., KUO, F.-Y. & SUN, P.-C. An intention model-based study of software piracy. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences, 5-8 January 1999. 1-8.
MALHOTRA, N. K. 2010. *Marketing Research: An Applied Orientation*, Prentice Hall.
MAPLE, C. & PHILLIPS, A. 2010. UK Security Breach Investigations Report: An Analysis of Data Compromise Cases. *7Safe*

MCCARTHY, B. 2002. New economics of sociological criminology. *Annual Review of Sociology,* 28**,** 417-442.
MCFADZEAN, E., EZINGEARD, J.-N. & BIRCHALL, D. 2007. Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review,* 31**,** 622-660.
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.
MERHI, M. I. & AHLUWALIA, P. 2019. Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior,* 92**,** 37-46.
MOODY, G. D., SIPONEN, M. & PAHNILA, S. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly,* 42**,** 285-A22.
MOORE, S. & KEEN, E. 2018. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. SYDNEY, Australia: Gartner
MOYER, J. E. 2013. Managing mobile devices in hospitals: A literature review of BYOD policies and usage. *Journal of Hospital Librarianship,* 13**,** 197-208.
MUSE, L., HARRIS, S. G., GILES, W. F. & FEILD, H. S. 2008. Work‐life benefits and positive organizational behavior: is there a connection? *Journal of Organizational Behavior,* 29**,** 171-192.
MYERS, M. D. 2009. *Qualitative Research in Business & Management,* Thousand Oaks, CA, SAGE.
MYYRY, L., SIPONEN, M., PAHNILA, S., VARTIAINEN, T. & VANCE, A. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems,* 18**,** 126-139.
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) 2003. Special Publication 800-59: Guideline for Identifying an Information System as a National Security System.
NG, B.-Y., KANKANHALLI, A. & XU, Y. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems,* 46**,** 815-825.
NOTANI, A. S. 1998. Moderators of Perceived Behavioral Control's Predictiveness in the Theory of Planned Behavior: A Meta-Analysis. *Journal of Consumer Psychology,* 7**,** 247-271.

OLSON-BUCHANAN, J. B. & BOSWELL, W. R. 2006. Blurring boundaries: Correlates of integration and segmentation between work and nonwork. *Journal of Vocational behavior,* 68**,** 432-445.
ONWUDIWE, H. D., ODO, J. & ONYEOZILI, E. C. 2005. Encyclopedia of Prisons & Correctional Facilities. Thousand Oaks, California: SAGE.
PADAYACHEE, K. 2012. Taxonomy of compliant information security behavior. *Computers & Security,* 31**,** 673-680.
PAHNILA, S., KARJALAINEN, M. & SIPONEN, M. Information Security Behavior: Towards Multi-Stage Models. PACIS 2013 Proceedings, 2013. 102.
PAHNILA, S., SIPONEN, M. & MAHMOOD, A. Employees' behavior towards IS security policy compliance. System Sciences, 2007a. HICSS 2007. 40th Annual Hawaii International Conference on, 3-6 January 2007a Hawaii. Hawaii: IEEE, 156b-156b.
PAHNILA, S., SIPONEN, M. & MAHMOOD, A. Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. PACIS 2007 Proceedings, 4 - 7 July 2007b New Zealand. New Zealand, 73.
PALANISAMY, R., NORMAN, A. A. & KIAH, M. L. M. 2020a. Compliance with bring your own device security policies in organizations: A systematic literature review. *Computers & Security,* 98**,** 101998.
PALANISAMY, R., NORMAN, A. A. & MAT KIAH, M. L. 2020b. BYOD Policy Compliance: Risks and Strategies in Organizations. *Journal of Computer Information Systems***,** 1-12.
PAOLACCI, G., CHANDLER, J. & IPEIROTIS, P. G. 2010. Running experiments on amazon mechanical turk. *Judgment and Decision Making,* 5**,** 411-419.
PAPAGEORGHIOU, A. T. 2020. The new normal. *BJOG: An International Journal of Obstetrics & Gynaecology,* 127**,** 779-780.
PARK, Y. & JEX, S. M. 2011. Work-home boundary management using communication and information technology. *International Journal of Stress Management,* 18**,** 133-152.
PEACE, A. G., GALLETTA , F. D. & THONG, Y. L. J. 2003. Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems,* 20**,** 153-177.
PONEMON INSTITUTE 2010. Access Governance Trends Survey: United States. Ponemon Institute LLC.
PONEMON INSTITUTE 2012. Cost of Cyber Crime Study: United States. Ponemon Institute LLC.
PONEMON INSTITUTE 2013. Cost of Data Breach Study: Global Analysis. Ponemon Institute LLC.
PONEMON INSTITUTE 2017a. Cost of Cyber Crime Study: Insights On The Security Investments That Make A Difference. Ponemon Institute LLC.
PONEMON INSTITUTE 2017b. Cost of Data Breach Study: Global Overview. Ponemon Institute LCC.
POSEY, C., BENNETT, R. J. & ROBERTS, T. L. 2011. Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security,* 30**,** 486-497.
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.
POTTER, C. & WATERFALL, G. 2012. Information security breaches survey. PWC.
PRIVACY RIGHTS CLEARINGHOUSE 2012. Data Breaches. Chronology of Data Breaches Database.
PRIVACY RIGHTS CLEARINGHOUSE 2018. Data Breaches. Chronology of Data Breaches Database.
PUHAKAINEN, P. & SIPONEN, M. 2010. IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY. *MIS Quarterly,* 34**,** 757-778.
RAJAB, M. & EYDGAHI, A. 2019. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security,* 80**,** 211-223.
RANDALL, D. M. & WOLFF, J. A. 1994. The time interval in the intention‐behaviour relationship: Meta‐analysis. *British Journal of Social Psychology,* 33**,** 405-418.
RHEE, H.-S., KIM, C. & RYU, Y. U. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security,* 28**,** 816-826.
RICHARDSON, R. 2011. 2010/2011 Computer Crime and Security Survey. Computer Security Institute.
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.

ROGERS, R. W. 1975. A Protection Motivation Theory Of Fear Appeals And Attitude Change. *Journal of Psychology,* 91**,** 93-114.
ROGERS, R. W. 1983. Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. *In:* CACIOPPO, J. & PETTY, R. (eds.) *Social Psychophysiology: A Sourcebook.* New York: Guilford Press.
ROGERS, R. W. & PRENTICE-DUNN, S. 1997. Protection Motivation Theory. *In:* GOCHMAN, D. S. (ed.) *Handbook of Health Behavior Research I: Personal and Social Determinants.* New York: Plenum Press.
ROSENSTOCK, I. M. 1974. Historical origins of the health belief model. *Health Education Monographs,* 2**,** 328-335.
SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A. & HERAWAN, T. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security,* 53**,** 65-78.
SANDERSON, C. A. & JEMMOTT, J. B. 1996. Moderation and Mediation of HIV-Prevention Interventions: Relationship Status, Intentions, and Condom Use Among College Students. *Journal of Applied Social Psychology,* 26**,** 2076-2099.
SASSE, M. A., BROSTOFF, S. & WEIRICH, D. 2001. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technology Journal,* 19**,** 122-131.
SAYAH, S. 2013. Managing work–life boundaries with information and communication technologies: The case of independent contractors. *New Technology, Work and Employment,* 28**,** 179-196.
SCOTLAND, J. 2012. Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching,* 5**,** 9-16.
SHARMA, S. & WARKENTIN, M. 2018. Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security***,** 87.
SHEERAN, P. & ORBELL, S. 1999. Implementation intentions and repeated behaviour: augmenting the predictive validity of the theory of planned behaviour. *European Journal of Social Psychology,* 29**,** 349-369.
SHEPPARD, B. H., HARTWICK, J. & WARSHAW, P. R. 1988. The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research,* 15**,** 325-343.
SHROPSHIRE, J. 2009. A canonical analysis of intentional information security breaches by insiders. *Information Management & Computer Security,* 17**,** 296-310.
SHROPSHIRE, J., WARKENTIN, M. & SHARMA, S. 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security,* 49**,** 177-191.
SIPONEN, M. 2005. An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems,* 14**,** 303-315.
SIPONEN, M., ADAM MAHMOOD, M. & PAHNILA, S. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management,* 51**,** 217-224.
SIPONEN, M. & OINAS-KUKKONEN, H. 2007. A Review of Information Security Issues and Respective Research Contributions. *Database for Advances in Information Systems,* 38**,** 60-80.
SIPONEN, M., PAHNILA, S. & MAHMOOD, A. Factors Influencing Protection Motivation and IS Security Policy Compliance. Innovations in Information Technology, 2006. 1-5.
SIPONEN, M., PAHNILA, S. & MAHMOOD, A. 2007. Employees' adherence to information security policies: an empirical study. *New Approaches for Security, Privacy and Trust in Complex Environments***,** 133-144.
SIPONEN, M., PAHNILA, S. & MAHMOOD, M. A. 2010. Compliance with Information Security Policies: An Empirical Investigation. *Computer,* 43**,** 64-71.
SIPONEN, M. & VANCE, A. 2010. neutralization: New Insights Into The Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly,* 34**,** 487-502.
SIPONEN, M., VANCE, A. & WILLISON, R. 2012. New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management,* 49**,** 334-341.
SKINNER, W. F. & FREAM, A. M. 1997. A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency,* 34**,** 495-518.
SMITH, J. 2010. Getting the Right Balance: Information Security and Information Access. *Legal Information Management,* 10**,** 51-54.

SMITH, S. & JAMIESON, R. 2006. DETERMINING KEY FACTORS IN E-GOVERNMENT INFORMATION SYSTEM SECURITY. *Information Systems Management,* 23**,** 23-32.
SOHRABI SAFA, N., VON SOLMS, R. & FURNELL, S. 2016. Information security policy compliance model in organizations. *Computers & Security,* 56**,** 70-82.
SOMMESTAD, T., HALLBERG, J., LUNDHOLM, K. & BENGTSSON, J. 2014. Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security,* 22**,** 42-75.
SOMMESTAD, T., KARLZÉN, H. & HALLBERG, J. 2015. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security,* 23**,** 200-217.
SON, J.-Y. 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management,* 48**,** 296-302.
STEELMAN, Z. R., LACITY, M. & SABHERWAL, R. 2016. Charting Your Organization's Bring-Your-Own-Device Voyage. *MIS Quarterly Executive,* 15.
STRAUB, D., BOUDREAU, M.-C. & GEFEN, D. 2004. VALIDATION GUIDELINES FOR IS POSITIVIST RESEARCH. *Communications of the Association for Information Systems,* 13**,** 380-427.
STRAUB, D. W. 1989. Validating Instruments in MIS Research. *MIS Quarterly,* 13**,** 147-169.
STRAUB JR, D. W. 1990. Effective IS Security: An Empirical Study. *Information Systems Research,* 1**,** 255-276.
SYKES, G. M. & MATZA, D. 1957. Techniques of neutralization: A theory of delinquency. *American Sociological Review,* 22**,** 664-670.
SYMANTEC 2019. Internet Security Threat Report.
TENAKOON, U. 2007. Impact of the use of communication technologies on the work-life balance of executive employees. *2007 Information Resources Management Association***,** 557-560.
THOMSON, G. 2012. BYOD: Enabling the chaos. *Network Security,* 2012**,** 5-8.
TOKUYOSHI, B. 2013. The security implications of BYOD. *Network Security,* 2013**,** 12-13.
TORTEN, R., REAICHE, C. & BOYLE, S. 2018. The impact of security awarness on information technology professionals' behavior. *Computers & Security,* 79**,** 68-79.
TSAI, H.-Y. S., JIANG, M., ALHABASH, S., LAROSE, R., RIFON, N. J. & COTTEN, S. R. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security,* 59**,** 138-150.
VAIDYA, R. 2018. Cyber Security Breaches Survey 2018: Statistical Release. London: Ipsos MORI Social Research Institute
VANCE, A., LOWRY, P. B. & EGGETT, D. 2013. Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems,* 29**,** 263-290.
VANCE, A. & SIPONEN, M. 2012. IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing,* 24**,** 21-41.
VANCE, A., SIPONEN, M. & PAHNILA, S. 2012. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management,* 49**,** 190-198.
VASUMATHI, A., MARY, T. S. & SUBASHINI, R. 2015. The impacts of emotional intelligence on work life balance: An empirical study among faculty members' performance in educational institutions at Tamil Nadu, India. *Pertanika Journal of Social Sciences and Humanities,* 23**,** 391-411.
VERIZON 2012. Data Breach Investigations Report.
VERIZON 2019. Data Breach Investigations Report.
VERIZON 2020. Data Breach Investigations Report.
WANG, Y., YUAN, K. & XU, T. Research on Architecture and Definition of Content Security. Communications and Intelligence Information Security (ICCIIS), 2010 International Conference on, 2010. NanNing,China, 64-68.
WARKENTIN, M., JOHNSTON, A. C. & SHROPSHIRE, J. 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems,* 20**,** 267-284.
WARKENTIN, M., JOHNSTON, A. C., SHROPSHIRE, J. & BARNETT, W. D. 2016. Continuance of protective security behavior: A longitudinal study. *Decision Support Systems,* 92**,** 25-35.
WILLIAMS, K. R. & HAWKINS, R. 1986. Perceptual Research on General Deterrence: A Critical Review. *Law & Society Review,* 20**,** 545-572.
WILLIS, D. 2014. Bring Your Own Device: The Results and the Future.

WORKMAN, M., BOMMER, W. H. & STRAUB, D. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior,* 24**,** 2799-2816.
WORKMAN, M. & GATHEGI, J. 2007. Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology,* 58**,** 212-222.
XIE, J., MA, H., ZHOU, Z. E. & TANG, H. 2018. Work-related use of information and communication technologies after hours (W_ICTs) and emotional exhaustion: A mediated moderation model. *Computers in Human Behavior,* 79**,** 94-104.
YAZDANMEHR, A. & WANG, J. 2016. Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems,* 92**,** 36-46.
YLIJOKI, O.-H. 2013. Boundary-work between work and life in the high-speed university. *Studies in Higher Education,* 38**,** 242-255.
YOO, C. W., SANDERS, G. L. & CERVENY, R. P. 2018. Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems,* 108**,** 107-118.
YOON, C. & KIM, H. 2013. Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People,* 26**,** 401-419.
ZHANG, J., REITHEL, B. J. & LI, H. 2009a. Impact of perceived technical protection on security behaviors. *Information Management & Computer Security,* 17**,** 330-340.
ZHANG, L., SMITH, W. W. & MCDOWELL, W. C. 2009b. Examining Digital Piracy: Self-Control, Punishment, and Self-Efficacy. *Information Resources Management Journal,* 22**,** 24-44.
ZISSIS, D. & LEKKAS, D. 2011. Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly,* 28**,** 239-251.

APPENDIXES

APPENDIX A: Comparison Between Positive and Negative Employees Information Security Behavior Studies

Total No. of Studies	**Positive Studies**	**No. of Positive Studies**	**Negative Studies**	**No. of Negative Studies**
82	Lee et al. (2004); Chan et al. (2005); Siponen et al. (2006); Pahnila et al. (2007b); Pahnila et al. (2007a); Siponen et al. (2007); Boss et al. (2009); Bulgurcu et al. (2009); Herath and Rao (2009b); Herath and Rao (2009a); Myyry et al. (2009); Ng et al. (2009); Rhee et al. (2009); Zhang et al. (2009a); Bulgurcu et al. (2010b); Bulgurcu et al. (2010a); Johnston and Warkentin (2010); Siponen et al. (2010); Son (2011); Chen (2012); Hu et al. (2012); Ifinedo (2012); Vance et al. (2012); Al-Omari et al. (2013); Pahnila et al. (2013); Yoon and Kim (2013); Ifinedo (2014); Siponen et al. (2014); Boss et al. (2015); Humaidi and Balakrishnan (2015); Johnston et al. (2015); Posey et al. (2015); Safa et al. (2015); Shropshire et al. (2015); Sommestad et al. (2015); Hanus and Wu (2016); Ifinedo (2016); Rocha Flores and Ekstedt (2016); Sohrabi Safa et al. (2016); Warkentin et al. (2016); Yazdanmehr and Wang (2016); Aurigemma and Mattson (2017); Bélanger et al. (2017); Burns et al. (2017); Han et al. (2017); Menard et al. (2017); Amankwa et al. (2018); Chen et al. (2018); Chua et al. (2018); Hwang and Cha (2018); Sharma and Warkentin (2018); Torten et al. (2018); Yoo et al. (2018); Ahmad et al. (2019); Dodel and Mesch (2019); Li et al. (2019); Rajab and Eydgahi (2019)	57	Straub Jr (1990); Harrington (1996); Skinner and Fream (1997); D'Arcy and Hovav (2007); Dugo (2007); Workman and Gathegi (2007); Workman et al. (2008); D'Arcy and Hovav (2009); D'Arcy et al. (2009); Siponen and Vance (2010); Guo et al. (2011); Hu et al. (2011); Posey et al. (2011); Cox (2012); Guo and Yuan (2012); Vance and Siponen (2012); Barlow et al. (2013); Cheng et al. (2013); D'Arcy et al. (2014); Johnston et al. (2016); Alshare et al. (2018); Kajtazi et al. (2018); Moody et al. (2018); Lankton et al. (2019); Merhi and Ahluwalia (2019)	25

APPENDIX B: Descriptions and Results of Most Used Concepts In Employees' Information Security Behavioral Studies

			Positive Security Behaviors				**Negative Security Behaviors**			
			Relationship with Intention		**Relationship with Behavior**		**Relationship with Intention**		**Relationship with Behavior**	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Self-Efficacy	35	Employees' beliefs in their own ability to perform the behavior of complying with the information security policy	17 Applications Siponen et al. (2006); Pahnila et al. (2007b); Siponen et al. (2007); Boss et al. (2009); Herath and Rao (2009b); Bulgurcu et al. (2010a); Johnston and Warkentin (2010); Siponen et al. (2010); Son (2011); Ifinedo (2012); Vance et al. (2012); Al-Omari et al. (2013); Siponen et al. (2014); Johnston et al. (2015); Rocha Flores and Ekstedt (2016); Warkentin et al. (2016); Yoo et al. (2018)	6 Applications Pahnila et al. (2013); Ifinedo (2014); Boss et al. (2015); Bélanger et al. (2017); Menard et al. (2017); Rajab and Eydgahi (2019).	9 Applications Chan et al. (2005); Ng et al. (2009); Rhee et al. (2009); Safa et al. (2015); Hanus and Wu (2016); Torten et al. (2018); Ahmad et al. (2019); Dodel and Mesch (2019); Li et al. (2019)	-	1 Application Moody et al. (2018)	1 Application Johnston et al. (2016)	1 Application Workman et al. (2008)	-

			Positive Security Behaviors				Negative Security Behaviors			
			Relationship with Intention		Relationship with Behavior		Relationship with Intention		Relationship with Behavior	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Response Efficacy	26	Employees' beliefs in their own ability to perform the behavior to comply with the information security policy	14 Applications Siponen et al. (2006); Siponen et al. (2007); Herath and Rao (2009a); Johnston and Warkentin (2010); Ifinedo (2012); Vance et al. (2012); Pahnila et al. (2013); Boss et al. (2015); Johnston et al. (2015); Posey et al. (2015); Sommestad et al. (2015); Burns et al. (2017); Menard et al. (2017); Rajab and Eydgahi (2019)	5 Applications Pahnila et al. (2007b); Siponen et al. (2010); Siponen et al. (2014); Boss et al. (2015); Warkentin et al. (2016)	4 Applications Posey et al. (2015); Hanus and Wu (2016); Torten et al. (2018); Li et al. (2019)	-	-	2 Applications Johnston et al. (2016); Moody et al. (2018)	1 Application Workman et al. (2008)	-

			Positive Security Behaviors				Negative Security Behaviors			
			Relationship with Intention		Relationship with Behavior		Relationship with Intention		Relationship with Behavior	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Attitude	23	Employees' evaluation of performing a behavior to comply with the information security policy in terms of favorability and the expected outcome	16 Applications Pahnila et al. (2007a); Bulgurcu et al. (2009); Zhang et al. (2009a); Bulgurcu et al. (2010a); Hu et al. (2012); Ifinedo (2012); Al-Omari et al. (2013); Yoon and Kim (2013); Ifinedo (2014); Siponen et al. (2014); Sommestad et al. (2015); Rocha Flores and Ekstedt (2016); Sohrabi Safa et al. (2016); Aurigemma and Mattson (2017); Bélanger et al. (2017); Amankwa et al. (2018)	2 Applications Herath and Rao (2009b); Rajab and Eydgahi (2019)	1 Application Safa et al. (2015)	-	4 Applications Dugo (2007); Guo et al. (2011); Cox (2012); Moody et al. (2018)	-	-	-

			Positive Security Behaviors				Negative Security Behaviors			
			Relationship with Intention		Relationship with Behavior		Relationship with Intention		Relationship with Behavior	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Injunctive Norms	22	Employees' beliefs about the expectation of significant others (e.g. executives, colleagues, peers etc.) of them when it comes to complying with the information security policy	13 Applications Pahnila et al. (2007b); Pahnila et al. (2007a); Herath and Rao (2009b); Herath and Rao (2009a); Bulgurcu et al. (2010a); Siponen et al. (2010); Hu et al. (2012); Ifinedo (2012); Al-Omari et al. (2013); Ifinedo (2014); Siponen et al. (2014); Rocha Flores and Ekstedt (2016); Aurigemma and Mattson (2017)	3 Applications Zhang et al. (2009a); Bélanger et al. (2017); Rajab and Eydgahi (2019)	1 Application Safa et al. (2015)	-	5 Applications Dugo (2007); Cox (2012); Guo and Yuan (2012); Cheng et al. (2013); Moody et al. (2018)	-	-	-

			Positive Security Behaviors				Negative Security Behaviors			
			Relationship with Intention		Relationship with Behavior		Relationship with Intention		Relationship with Behavior	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Perceived Threat Severity	21	Employees' assumption of the magnitude of harm that may be caused by the threatened event if they didn't comply with the information security policy	10 Applications Siponen et al. (2006); Ifinedo (2012); Vance et al. (2012); Pahnila et al. (2013); Siponen et al. (2014); Boss et al. (2015); Johnston et al. (2015); Sommestad et al. (2015); Warkentin et al. (2016); Burns et al. (2017)	4 Applications Boss et al. (2015); Posey et al. (2015); Menard et al. (2017); Rajab and Eydgahi (2019)	2 Applications Posey et al. (2015); Torten et al. (2018)	2 Applications Hanus and Wu (2016); Li et al. (2019)	-	2 Applications Johnston et al. (2016); Moody et al. (2018)	1 Application Workman et al. (2008)	-
Perceived Severity of Sanctions	20	Employees' beliefs of harshness of punishment for not complying with the information security policy	7 Applications Siponen et al. (2007); Herath and Rao (2009b); Herath and Rao (2009a); Chen (2012); Johnston et al. (2015); Ifinedo (2016); Chen et al. (2018)	5 Applications Pahnila et al. (2007a); Son (2011); Ifinedo (2014); Johnston et al. (2015); Rajab and Eydgahi (2019)	1 Application Pahnila et al. (2007b)	-	3 Applications D'Arcy et al. (2009); Cheng et al. (2013); Johnston et al. (2016)	2 Applications Hu et al. (2011); Vance and Siponen (2012)	2 Application Skinner and Fream (1997); Alshare et al. (2018)	-

			Positive Security Behaviors				Negative Security Behaviors			
			Relationship with Intention		Relationship with Behavior		Relationship with Intention		Relationship with Behavior	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Perceived Threat Vulnerability	19	Employees' beliefs of the probability that a threatening event may occur if they do not comply with the information security policy	7 Applications Siponen et al. (2006); Ifinedo (2012); Pahnila et al. (2013); Siponen et al. (2014); Sommestad et al. (2015); Warkentin et al. (2016); Rajab and Eydgahi (2019)	5 Applications Vance et al. (2012); Pahnila et al. (2013); Boss et al. (2015); Johnston et al. (2015); Menard et al. (2017)	3 Applications Ng et al. (2009); Torten et al. (2018); Li et al. (2019)	1 Application Hanus and Wu (2016)	2 Applications Johnston et al. (2016); Moody et al. (2018)	-	1 Application Workman et al. (2008)	-
Response Cost	15	Employees' evaluation of the cost (e.g. time, effort, money, etc.) associated with either performing or not performing the behavior to comply with the information security policy	7 Applications Vance et al. (2012); Boss et al. (2015); Posey et al. (2015); Sommestad et al. (2015); Burns et al. (2017); Chen et al. (2018); Rajab and Eydgahi (2019)	2 Applications Ifinedo (2012); Menard et al. (2017)	1 Application Torten et al. (2018)	2 Applications Posey et al. (2015); Hanus and Wu (2016)	-	2 Applications Johnston et al. (2016); Moody et al. (2018)	1 Application Workman et al. (2008)	-
Perceived Certainty of Sanctions	14	Employees' assumptions of the probability of being punished for not complying with the information security policy	3 Applications Herath and Rao (2009b); Herath and Rao (2009a); Johnston et al. (2015)	5 Applications Son (2011); Ifinedo (2014); Johnston et al. (2015); Ifinedo (2016); Rajab and Eydgahi (2019)	-	-	1 Application Johnston et al. (2016)	4 Applications D'Arcy et al. (2009); Siponen and Vance (2010); Hu et al. (2011); Cheng et al. (2013)	-	1 Application Skinner and Fream (1997)

			Positive Security Behaviors				Negative Security Behaviors			
			Relationship with Intention		Relationship with Behavior		Relationship with Intention		Relationship with Behavior	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Rewards	12	Employees' beliefs of the benefits they will gain by complying with the information security policy, whether these benefits are tangible or intangible, or intrinsic or extrinsic.	4 Applications Chen (2012); Vance et al. (2012); Posey et al. (2015); Burns et al. (2017)	2 Applications Siponen et al. (2014); Posey et al. (2015)	1 Application Posey et al. (2015)	4 Applications Pahnila et al. (2007b); Pahnila et al. (2007a); Siponen et al. (2010); Posey et al. (2015)	1 Application Moody et al. (2018)	-	-	-
Perceived Behavioral Control	10	Employees' beliefs as to whether they have the control to decide whether or not to comply with the information security policy and have the required capabilities to perform it.	4 Applications Zhang et al. (2009a); Hu et al. (2012); Sommestad et al. (2015); Aurigemma and Mattson (2017)	1 Application Rajab and Eydgahi (2019)	-	1 Application Safa et al. (2015)	3 Applications Dugo (2007); Cox (2012); Moody et al. (2018)	-	1 Application Cox (2012)	-
Moral Norm	8	Employees' perception of how moral it is to comply with the information security policy.	2 Applications Al-Omari et al. (2013); Yoon and Kim (2013)	-	-	-	6 Applications D'Arcy and Hovav (2009); D'Arcy et al. (2009); Guo and Yuan (2012); Vance and Siponen (2012); D'Arcy et al. (2014); Lankton et al. (2019)	-	-	-

			Positive Security Behaviors				Negative Security Behaviors			
			Relationship with Intention		Relationship with Behavior		Relationship with Intention		Relationship with Behavior	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Descriptive Norm	5	Employees' beliefs whether the significant others (e.g. executives, colleagues, peers etc.) would or would not comply with the information security policy if they were in the same situation.	3 Applications Herath and Rao (2009b); Herath and Rao (2009a); Chen et al. (2018)	-	-	-	1 Application Cheng et al. (2013)	-	1 Application Merhi and Ahluwalia (2019)	-
Perceived Celerity of Sanctions	4	Employees' beliefs of how fast the punishment for non-compliance with information security policy will occur.	-	2 Applications Johnston et al. (2015); Rajab and Eydgahi (2019)	-	-	-	1 Application Hu et al. (2011)	1 Application Alshare et al. (2018)	-
Shame	4	Employees' feeling of embarrassment if others find out that they are not complying with the information security policy.	-	-	-	-	Moody et al. (2018)	Siponen and Vance (2010) Hu et al. (2011) Moody et al. (2018)	-	-

			Positive Security Behaviors				Negative Security Behaviors			
			Relationship with Intention		Relationship with Behavior		Relationship with Intention		Relationship with Behavior	
Name	**Usages in Information Security Applications**	**Definition in Information Security Studies**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**	**Supported**	**Not Supported**
Habit	3	Information Security Behaviors that are being performed by the employees' unconsciously or automatically without mindful instructions or consciousness.	1 Application Pahnila et al. (2007a)	-	-	-	1 Application Moody et al. (2018)	1 Application Moody et al. (2018)	-	-

APPENDIX C: Measurement Items

#	Construct	Model	Theory	Item	Derived from
1	Scenario Realism 1	Both	Scenario Realism Items	How believable do you think the above scenario is not believable:___1___:___2___:___3___:___4___:___5___:___6___:___7___: believable	New
2	Scenario Realism 2	Both	Scenario Realism Items	The above scenario is a realistic one Not realistic:___1___:___2___:___3___:___4___:___5___:___6___:___7___: realistic	New
3	Scenario Realism 3	Both	Scenario Realism Items	I could imagine a similar scenario taking place at work disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___: strongly agree	New
4	Scenario Realism 4	Both	Scenario Realism Items	The situation described in the scenario could occur disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___: strongly agree	New
5	Device Ownership	Model 1	BYOD Contextual Factor	In this scenario, John was using a. his own laptop b. company owned laptop	New
6	Sensitivity Company Data	Model 1	BYOD Contextual Factor	According to this scenario, John was aware that the laptop he is using contains a. company Owned Sensitive data b. company Owned Insensitive data	New
7	Sensitivity Personal Data	Model 1	BYOD Contextual Factor	Per this scenario, John was aware that the laptop he is using contains a. his personal Sensitive data b. his personal Insensitive data	New
8	Place	Model 1	BYOD Contextual Factor	John was using the laptop a. at home b. at work	New
9	Activity	Model 1	BYOD Contextual Factor	In this scenario, John was using the laptop to a. perform personal task b. perform company task	New
10	Time	Model 1	BYOD Contextual Factor	John was using the laptop a. after working hours b. during working hours	New
11	Work Life Balance 3	Model 1	Work Life Balance	If am using the laptop in the same scenario, then I believe that am in my work domain:___1___:___2___:___3___:___4___:___5___:___6___:___7___: life domain	New
12	Work Life Balance 4	Model 1	Work Life Balance	In provide scenario, John usage of the laptop feel more like he is in his work domain:___1___:___2___:___3___:___4___:___5___:___6___:___7___: life domain	New
13	Self-Efficacy 1	Model 2	Protection Motivation Theory	For me to comply with the requirements of my organization's information security policy would be very difficult:___1___:___2___:___3___:___4___:___5___:___6___:___7___:very easy	Sheeran and Orbell (1999)
14	Self-Efficacy 2	Model 2	Protection Motivation Theory	If I want to I will easily be able to comply with the requirements of my organization's information security policy strongly disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___:strongly agree	Sheeran and Orbell (1999); Al-Omari et al. (2013)
15	Self-Efficacy 3	Model 2	Protection Motivation Theory	The number of external influences that may prevent me from complying with the requirements of my organization's information security policy are numerous:___1___:___2___:___3___:___4___:___5___:___6___:___7___:none at all	Sheeran and Orbell (1999)
16	Self-Efficacy 4	Model 2	Protection Motivation Theory	How much control do you think you have over your ability to comply with the requirements of the information security policy in your organization? absolutely no control:___1___:___2___:___3___:___4___:___5___:___6___:___7___:complete control	Sheeran and Orbell (1999)

#	Construct	Model	Theory	Item	Derived from
17	Perceived Threat Severity 1	Model 2	Protection Motivation Theory	I believe that protecting my organization's information is unimportant:___1___:___2___:___3___:___4___:___5___:___6___:___7___:important	Ifinedo (2012)
18	Perceived Threat Severity 2	Model 2	Protection Motivation Theory	Having someone successfully attack and damage my computer (at work) is harmless:___1___:___2___:___3___:___4___:___5___:___6___:___7___:harmful	Ifinedo (2012)
19	Perceived Threat Severity 3	Model 2	Protection Motivation Theory	Threats to the security of my organization's information are harmless:___1___:___2___:___3___:___4___:___5___:___6___:___7___:harmful	Ifinedo (2012)
20	Perceived Threat Severity 4	Model 2	Protection Motivation Theory	I view information security attacks on my organization as harmless:___1___:___2___:___3___:___4___:___5___:___6___:___7___:harmful	Ifinedo (2012)
21	Perceived Threat Vulnerability 1	Model 2	Protection Motivation Theory	I know my organization could be vulnerable to security breaches if I don't adhere to the requirements of my organization's information security policy strongly disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___:strongly agree	Ifinedo (2012)
22	Perceived Threat Vulnerability 2	Model 2	Protection Motivation Theory	I could fall victim to a malicious attack if I fail to comply with the requirements of my organization's information security policy strongly disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___:strongly agree	Ifinedo (2012)
23	Perceived Threat Vulnerability 3	Model 2	Protection Motivation Theory	I believe that trying to protect my company's information will reduce illegal access to it Strongly disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___:strongly agree	Ifinedo (2012)
24	Perceived Threat Vulnerability 4	Model 2	Protection Motivation Theory	My organization's data and resources may be compromised if I don't pay adequate attention to the requirements of my organization's information security policy Strongly disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___:strongly agree	Ifinedo (2012)
25	Reward 1	Model 2	Protection Motivation Theory	My pay raises and/or promotions depend on whether I comply with the requirements of my organization's information security policy Not at All:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Very Much	Bulgurcu et al. (2010a)
26	Reward 2	Model 2	Protection Motivation Theory	I will receive personal mention in oral or written assessment reports if I comply with the requirements of my organization's information security policy Not at All:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Very Much	Bulgurcu et al. (2010a)
27	Reward 3	Model 2	Protection Motivation Theory	I will be given monetary or non-monetary rewards if I comply with the requirements of my organization's information security policy Not at All:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Very Much	Bulgurcu et al. (2010a)
28	Reward 4	Model 2	Protection Motivation Theory	My receiving tangible or intangible rewards are tied to whether I comply with the requirements of my organization's information security policy Not at All:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Very Much	Bulgurcu et al. (2010a)
29	Response Efficacy 1	Model 2	Protection Motivation Theory	The preventative measures available to me to prevent people from damaging my information system at work are Inadequate:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Adequate	Workman et al. (2008); Ifinedo (2012)
30	Response Efficacy 2	Model 2	Protection Motivation Theory	The effectiveness of available measures to protect my organization's information from security violations are Ineffective:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Effective	Workman et al. (2008); Ifinedo (2012)
31	Response Efficacy 3	Model 2	Protection Motivation Theory	Every employee can make a difference when it comes to helping to secure the organization's Information Security. Strongly Disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Strongly Agree	Herath and Rao (2009b)
32	Response Efficacy 4	Model 2	Protection Motivation Theory	If I follow the organization IS security policies, I can make a difference in helping to secure my organization's IS. Strongly Disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Strongly Agree	Herath and Rao (2009b)

#	Construct	Model	Theory	Item	Derived from
33	Response Cost 1	Model 2	Protection Motivation Theory	Enabling information systems security measures in my organization is/would be time consuming Strongly disagree:___1___:___2___:___3___:___4___:___5___:___6___:___7___:Strongly agree	Ifinedo (2012)
34	Response Cost 2	Model 2	Protection Motivation Theory	The impact to my work from recommended security measures exceeds benefits:___1___:___2___:___3___:___4___:___5___:___6___:___7___:outweighed by benefits	Workman et al. (2008)
35	Response Cost 3	Model 2	Protection Motivation Theory	The inconvenience to implement recommended security measures exceeds benefits:___1___:___2___:___3___:___4___:___5___:___6___:___7___:outweighed by benefits	Workman et al. (2008)
36	Response Cost 4	Model 2	Protection Motivation Theory	The cost to implement recommended security measures exceeds benefits:___1___:___2___:___3___:___4___:___5___:___6___:___7___:outweighed by benefits	Workman et al. (2008)
37	Intention 1	Model 2	Protection Motivation Theory	I would follow the requirements of my organization's information security policy whenever possible very unlikely-very likely	Ifinedo (2012)
38	Intention 2	Model 2	Protection Motivation Theory	I am likely to follow the requirements of my organization's information security policy in the future agree-disagree	Ifinedo (2012)
39	Intention 3	Model 2	Protection Motivation Theory	It is possible that I will comply with the requirements of my organization's information security policy to protect the organization's information systems agree-disagree	Ifinedo (2012)
40	Gender	Both	Control	Gender a. Male b. Female	Bulgurcu et al. (2010a)
41	Age	Both	Control	Age a. Under 20 b. 20–25 c. 26–35 d. 36–45 e. 46–55 f. 56–65 g. 66 and above	Bulgurcu et al. (2010a)
42	Marital Status	Both	Control	Marital Status a. Married b. Widowed c. Divorced d. Separated e. Never married	New
43	Education	Both	Control	Highest level of education a. Less than high school b. High school degree c. University or Bachelor's degree d. Master's Degree e. Doctorate's Degree	Johnston et al. (2015)
44	Experience	Both	Control	Total Years of experience? a. Less than 6 months b. 6 months to 12 months c. More than 1 year to 2 years d. More than 2 years to 5 years e. More than 5 years to 10 years f. More than 10 years	Johnston et al. (2015)
45	Position	Both	Control	Current Rank (position) in your organization a. Top management personnel b. Mid-Level personnel c. Junior Staff	Ifinedo (2014)

#	Construct	Model	Theory	Item	Derived from
46	Organization Size	Both	Control	Size of your Organization a. Fewer than 100 b. 100-499 c. 500-999 d. 1,000-4,999 e. 5,000-10,000 f. More than 10,000	Bulgurcu et al. (2010a)
47	Industry	Both	Control	Organization Industry a. Education b. Financial Services c. Government d. Food/Beverage/CPG e. Health Care f. Manufacturing g. Nonprofit h. Medical, Bio-Technology, Pharmacology i. Real Estate j. Services k. Information Technology l. Telecommunications m. Travel n. Wholesale/Retail o. Other _____	Bulgurcu et al. (2010a)
48	Job Role	Both	Control	Job role a. IT b. Non-IT	Herath and Rao (2009b)
49	Tenure	Both	Control	How long have you been with your current organization? a. Less than 3 Months b.3 months to 6 months c. More than 6 months to 12 months d. More than 12 months to 60 months e. More than 60 months	Son (2011)
50	IT Knowledge	Both	Control	Knowledge of computers and IT low :___1___:___2___:___3___:___4___:___5___:___6___:___7___: high	Bulgurcu et al. (2010a)