UNDERSTANDING EMPLOYEE NON-MALICIOUS INTENTIONAL AND UNINTENTIONAL INFORMATION SECURITY MISBEHAVIORS

By

FOROUGH NASIRPOURI SHADBAD

Bachelor of Science in Physics
University of Tabriz
Iran
2008

Master of Science in Physics
University of Tabriz
Iran
2011

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
DOCTOR OF PHILOSOPHY
May, 2021

UNDERSTANDING EMPLOYEE NON-MALICIOUS

INTENTIONAL AND UNINTENTIONAL

INFORMATION SECURITY MISBEHAVIORS

Dissertation Approved:

Dr. David Biros

Dissertation Adviser

Dr. Corey Baham

Dr. Obi Ogbanufe

Dr. Bryan Edwards

ACKNOWLEDGEMENTS

During my PhD journey, many helped and supported me to achieve my goals. I want to take a moment and thank them.

I am so grateful to my advisor, Dr. David Biros, for his dedicated support. Without his insightful guidance and invaluable advice, I would not have made it through this challenging experience. Dr. Biros continuously provided encouragement and was always willing and enthusiastic in any way he could throughout the multiple research projects. His support is not limited to only research discussions. He was always available to give me career advice and to provide the right direction where it is the best for me. I learned a lot from him about how to become successful in my future academic career.

I would also like to thank my committee members, Dr. Baham, Dr. Ogbanufe, and Dr. Edwards, for providing insightful comments for my research projects. Furthermore, I want to express my gratitude to the entire MSIS community of the Spears School of Business at OSU, who played important roles in this adventure.

I would also like to thank my parents for their love and support throughout my life. They gave me strength and encouragement to reach this point. My brother Farzad and my sisters, Faranak and Farzaneh, deserve my wholehearted thanks as well. Finally, last but not the least, I must thank my husband, Afshin. I find it difficult to thank him enough for all that he has done for me. He is my best friend and an amazing husband. Without his sunny optimism, love, and support, I would be lost through the ups and downs of this journey. I believe it seems right that I dedicate this dissertation to him.

Name: FOROUGH NASIRPOURI SHADBAD

Date of Degree: MAY, 2021

Title of Study: UNDERSTANDING EMPLOYEE NON-MALICIOUS INTENTIONAL AND UNINTENTIONAL INFORMATION SECURITY MISBEHAVIORS

Major Field: BUSINESS ADMINISTRATION

Abstract: Digitization has given rise to information system security (ISS) risks since the adoption of new technologies (e.g., IoT and multi-cloud environments) has increased vulnerabilities to ISS threats. The behavioral ISS literature depicts employees within organizations (insiders) as a major information security threat. Previous research extensively investigated insiders' intentional ISS misbehaviors. However, a growing number of security incidents by non-malicious insiders implies that potential factors influencing employees' non-compliance behaviors with information security policies (ISPs) are yet to be addressed. To this end, we conduct four (four essays) to understand why employees violate ISPs. Two studies investigate factors that lead to non-malicious intentional ISP violations. The other two studies explore how and why non-malicious unintentional ISP violations occur. Drawing on the person-technology fit model, essay 1 investigates how employees' interaction with information technology (IT) increases ISS vulnerabilities. This essay sheds light on the impact of one understudied aspect of IT use-technostress, on employees' non-malicious ISP violation intentions. Essay 2 relies on organizational role theory and explains stress resulting from role expectations, including intra-role activities (e.g., job tasks) and extra-role activities (e.g., ISS requirements) could cause ISP non-compliance behaviors. To distinguish non-malicious intentional insiders from unintentional insiders, Essay 3 employs the dual-system theory to describe the mechanism of employees' decision-making process to comply (or not comply) with ISPs and aims to investigate the impact of some personality traits like risk-taking behaviors, impulsivity, and curiosity on employees' ISS misbehaviors. Finally, to explore unknown factors influencing non-compliance behaviors with ISPs (e.g., individual, organizational), essay 4 proposes an in-depth qualitative approach to distinguish non-malicious intentional and unintentional ISS misbehaviors and identify potential causes rooted in each type of misbehavior. Overall, the dissertation highlights the importance of individual differences in perceptions of technostress, role stress, and personality traits. Moreover, it differentiates the nature of ISP violations based on the intents of employees and challenges the existing knowledge and theoretical frameworks regarding insiders' information security behaviors at the workplace. In doing so, proposed theoretical models are assessed empirically by utilizing data (both interviews and online surveys) from a sample of employees from different organizations.

TABLE OF CONTENTS

Chapter Page

Chapter Page

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

CHAPTER I

OVERVIEW

Information system security (ISS) is increasingly essential for organizations because security breaches are associated with monetary damage and loss of credibility (Cavusoglu, Cavusoglu, & Raghunathan, 2004). Despite various strategies that organizations consider to invest heavily in information security assets and infrastructure, statistical analyses show that the number of data breaches and the volume of exposed records in the US has been increasing in recent years (J. Clement, 2019), mainly rooted in human factors (Bellika, Makhlysheva, & Bakkevoll, 2018; IBM Global technology Service, 2014) implying that employees are the weakest link in the ISS and are responsible for the majority of breaches.

Despite past beliefs that outsiders (e.g., hackers) are the main reason for security breaches, insiders or internal employees are labeled as the weakest link in cybersecurity as they account for more than 50% of security violations reported by Baker et al. (2010) and remain the top source of security incidents (Loch, Carr, & Warkentin, 1992a; PWC, 2018). Except for malicious insider threats (Liang, Biros, & Luse, 2016), where individuals with harmful intentions deliberately attempt to hack or steal data for personal gains, insiders may violate information security policies (ISPs) non-maliciously in two ways: intentionally and unintentionally. Non-malicious intentional (NMI) deviant behaviors are defined as security violations performed consciously against the organizational ISPs with no malicious intent to cause destructions (K. H. Guo, Y. Yuan, N. P. Archer, & C. E. Connelly, 2011a). For example, writing down a password or sharing with a colleague, delayed backups, and installing unauthorized software are NMI. Non-malicious unintentional violations are those end-users' behaviors performed unconsciously and inadvertently without harmful intentions (Ayyagari, 2012). Accidental modification

of software, negligence, and ignorance, accidental clicks on phishing emails, and mis-delivery of sensitive data are examples of such misbehaviors. CSI Survey and other industry reports on information security incidents found that most of the security incidents belong to the non-malicious (intentional and unintentional) human behaviors (Bureau, 2013; Identity Theft Resource Center, 2019; Mahmmod Sher-Jan, 2018; Richard, 2010).

Scholars have devoted significant efforts to understanding why individuals deviate from best security practices or fail to comply with the ISPs (e.g., not locking down a computer while stepping away, writing down a password). In ISS literature, several theories have been applied to study employees security-related behaviors, such as the theory of planned behavior, deterrence theory, motivation-protection theory, neutralization theory, and rational choice theory (Bulgurcu, Cavusoglu, & Benbasat, 2010; Cox, 2012; D'arcy & Herath, 2011; D'Arcy, Hovav, & Galletta, 2009; Ifinedo, 2012; Karjalainen & Siponen, 2011; Li, Zhang, & Sarathy, 2010; M. Siponen & A. Vance, 2010; Straub Jr, 1990; Warkentin, Johnston, Shropshire, & Barnett, 2016). The purpose of applying these theories (and others) is to identify contributed factors or determinants of employees' intentional non-compliance behavior with ISPs. They mainly found that attitude, personal norms, ethics, normative beliefs, punishments, rewards expectancy, perceived formal and informal risk, self-efficacy, and information security training and awareness programs are the key factors determining what degree employees comply with ISP.

Despite the growing literature, there are some unanswered questions regarding individual differences in terms of their perception of stress regarding their role expectations and interactions with different types of technology. Furthermore, existing studies have not distinguished non-malicious intentional insiders from non-malicious unintentional insiders to provide empirical insights into unintentional insiders' motives and root causes. We address the existing research gap in four essays.

The advent of new technologies like ubiquities technologies, IoT, AI, and information and communication technologies (ICTs) has increased vulnerabilities to ISS threats (Liang & Xue, 2009a;

Loch, Carr, & Warkentin, 1992b). On the other side, IT use is associated with stress perception in individuals known as technostress, which reduces their job-related performance (Tarafdar, Tu, Ragu-Nathan, & Ragu-Nathan, 2007a). Given that employees are recognized as a major information security threat, it makes sense to investigate how technostress resulting from employees' constant interaction with IT influences the likelihood of security incidents. Thus, essay 1 focuses on the impact of technostress on employees' non-malicious ISP violations.

In addition to IT use, studies indicate that stress might be observed due to job role expectations and could reduce employee job performance (Igbaria & Siegel, 1992). Since many organizations require their employees to perform security-related tasks, employees might perceive some stress rooted in their role expectations due to role-ambiguity, role-conflict, and role-overload, known as role-stressors. These role-stressors might cause employees to endeavor to perform their role tasks and, in turn, provide favorable situations for them to neglect ISP requirements. Therefore, Essay 2 contributes to the behavioral information security literature by demonstrating the importance of role-stressors on employees' ISP compliance intention.

In essay 3, the dual system theory (Evans, 2003) was employed to better understand the differences between non-malicious intentional and unintentional insiders since individuals' decision-making behaviors follow two distinct automatic and rational cognitive systems. Due to the understudied aspect of personality traits in the context of ISP violation, we particularly look at employee's risk-taking behaviors, impulsivity, and curiosity as they are best described using dual-system theory (Trimpop, 1994). Hence, Essay 3 provides a theoretical model showing that employees with high risk-taking behaviors are more likely to engage in intentional and unintentional non-malicious ISP violations.

To differentiate contributed factors of non-malicious intentional from unintentional misbehaviors, Essay 4 proposes a broader approach to explore the possible factors that determine non-malicious ISP violations. An in-depth qualitative study will be conducted to investigate employee security-related

behaviors at the workplace to identify what reasons or factors might make employees violate ISPs unintentionally. Hence, essay 4 provides a comprehensive framework of the potential individual or organizational factors causing non-malicious unintentional ISP violations.

The four essays will add to the literature in several ways. Essay 1 extends the concept of technostress to the context of information security to unfold the negative impact of IT use on employees' non-malicious intention to violate ISPs. Essay 2 introduces organizational role theory as a theoretical lens to investigate how role stressors might be destructive for employee ISP compliance. Essay 3 utilizes dual system theory to provide a theoretical explanation and empirical support to highlights the role of risk-taking behaviors in enhancing the likelihood of employees' engagement in both intentional and unintentional non-malicious ISS misbehaviors. Finally, essay 4 provides a comprehensive framework of human and organizational factors to explain why employees are involved in unintentional ISP non-compliance. Figure 1.1 presents an overview of the dissertation, and Table 1.1 summarizes the research questions, theory and methods, and findings of each study. While four essays cover a wide range of topics, they all attempt to reveal rooted causes of employees' non-compliance behaviors with ISPs.

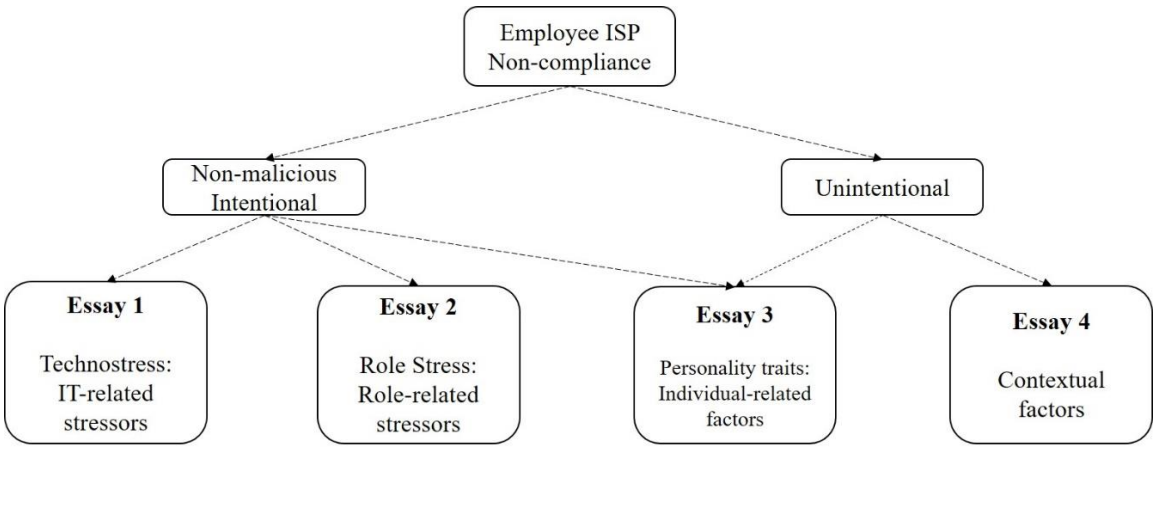

Figure 1.1 Map of Dissertation Essays

Table 1.1 Overview of the Dissertation Essays		
	Essay 1[1]	**Essay 2[2]**
Title	Technostress and its influence on employee ISP compliance	Understanding employee ISP compliance from role theory perspective
Research Question	a) Does technostress increase the likelihood of employees' intention to violate ISPs? b) Does techno-unreliability create technostress?	a) How does role stress relate to employee intention to comply with ISP, either directly or through organizational commitment? b) To what extent each type of role stress impact employee ISP compliance intention?
Theory	Person-Technology Fit	Organizational role theory
Method	Structural Equation Modeling	Structural Equation Modeling
Data	Survey	Survey
Findings	**a)** Technostress leads to employees' non-malicious ISP violation intentions. **b)** Among technostress creators, techno-complexity, techno-invasion, and techno-insecurity incline users to be more engaged in ISP non-compliance. **c)** The dimensionality of the technostress instrument was extended by adding techno-unreliability as a new technostress creator.	a) The stress of role expectations due to overload, ambiguity, and conflict leads to ISP non-compliance. b) Role stress indirectly contributes to lowering compliant behaviors through organizational commitment. c) Of the three, role-conflict contributed the most toward employee non-compliance intention.
	Essay 3	**Essay 4**
Title	Understanding non-malicious intentional and unintentional insiders using dual-system theory: an empirical validation	Understanding unintentional information security misbehaviors: A Qualitative approach
Research Question	a) Does employees' risk-taking behavior increase ISP violations? b) To what extent work-overload and security awareness moderate this relationship?	What types of contextual (e.g., individual and organizational) factors influence employees' non-malicious unintentional information security misbehavior? Why?
Theory	Dual-system Theory	N/A
Method	Structural Equation Modeling	Qualitative Approach
Data	Survey	Interview
Findings	a) Employees who have a high willingness to take risks in the workplace are more likely to violate ISPs either intentionally or unintentionally. b) Risk-taking behaviors mediate the relationship between non-malicious security misbehaviors and both impulsivity and curiosity. c) Perceived work-overload and information security awareness have positive and negative impacts on non-malicious ISP violations, respectively.	a) Determinants of non-malicious intentional are distinguishable from unintentional ISP violations. b) The preliminary results showed that some organizational and human factors provide favorable situations for insiders to perform both intentional and unintentional NISMs, such as risk-propensity and a lack of managerial practices (e.g., monitoring employee security-related behaviors).

[1] Shadbad, F. N., & Biros, D. (2020). Technostress and its Influence on Employee Information Security Policy Compliance. *Information Technology & People*. DOI: 10.1108/ITP-09-2020-0610

[2] Shadbad, F. N., & Biros, D. (2021). Understanding Employee Information Security Policy Compliance from Role Theory Perspective, *Journal of Computer Information Systems*, DOI: 10.1080/08874417.2020.1845584

CHAPTER II

TECHNOSTRESS AND ITS INFLUENCE ON EMPLOYEE INFORMATION SECURITY POLICY COMPLIANCE

2.1 Introduction

The 21st century is an era of complicated, advanced, and innovative information technology (IT) that has digitized our personal or professional lives. The advent of new and various types of IT like ubiquities technologies, IoT, AI, and information and communication technologies (ICTs) have revolutionized the nature of work and business processes (Forman, King, & Lyytinen, 2014). Subsequently, organizational effectiveness has been impacted dramatically in terms of productivity and employee performance (Bharadwaj, 2000; Brynjolfsson & Hitt, 2003). Nonetheless, scholars have discovered a dual nature of IT in which its use may have negative aspects and unintended consequences (D'Arcy, Gupta, Tarafdar, & Turel, 2014).

Along with the impact on effectiveness, digitization has enhanced the risk of information system security (ISS) violations since adoption in new technologies (e.g., IoT and multi-cloud environments) increases vulnerabilities to ISS threats (Liang & Xue, 2009b; Loch et al., 1992a). IT misuse such as email and network abuse is identified as an unintended negative result of reliance on IT and one of the leading security threats (D'Arcy et al., 2014). Although organizations employ counteraction strategies such as advanced security systems and information security policies (ISPs) (Baskerville & Siponen, 2002), security breaches are inevitable, and employees remain the top

source of ISS incidents because of ISP violations (Warkentin & Willison, 2009). ISP is defined as a set of guidelines and procedures that organizations require employees to follow in order to ensure security activities and proper use of organizational information and technology assets (Lowry & Moody, 2015). However, not all users comply with ISPs as prescribed (Besnard & Arief, 2004). They often rationalize and neutralize their behaviors to disregard ISPs based on a cost-benefit analysis of compliance (Bulgurcu et al., 2010; M. T. Siponen & A. Vance, 2010). Although countless studies have been devoted to identify contributing factors of non-compliant behaviors, further research is needed to explain employee ISP non-compliance. Furthermore, digitization has changed the daily work routine and has required employees to be more dependent on IT to accomplish tasks. However, using technology can be problematic since dependency on it creates stress in employees known as technostress (Tarafdar, Tu, Ragu-Nathan, & Ragu-Nathan, 2007b) where users feel that they have less energy, skill, or ability to deal with technology (i.e., feeling stressed due to the inability to cope with IT in a healthy manner). Users perceive some level of stress and frustration due to the technostress creators, including overload, complexity, invasion, uncertainty, and insecurity associated with IT use (Tarafdar et al., 2007b). In other words, using IT requires employees to perform more tasks and process more information, to adapt rapid and innovative technologies, to be continuously connected to IT, and to feel insecure and uncertain because of unfamiliarity and IT changes. Technostress negatively influences employees' performance and results in lower productivity, job satisfaction, organizational commitment, and in some cases increases their propensity to quit (Ragu-Nathan, Tarafdar, Ragu-Nathan, & Tu, 2008; Tarafdar, Tu, & Ragu-Nathan, 2010).

Nonetheless, the effect of technostress on employee security-related behaviors is an understudied concept. Some studies looked at both technostress and employee ISP violations in tandem (D'Arcy, Herath, & Shoss, 2014; Hwang & Cha, 2018). In a few studies, technostress has been extended to the context of ISS called security-related technostress where the objective of the study is to study

the employees' perceptions of stress caused by ISS requirements, either ISP or security technologies, on their security-related behaviors (D'Arcy et al., 2014; Hwang & Cha, 2018). Security-related technostress research focuses on the technological aspects of security systems or security requirements. For example, users might refuse to comply with ISPs if they found security tasks stressful due to complexity or uncertainty. However, the literature on behavioral ISS seems to lack consideration of the impact of IT itself on employees' extra-role activities like ISP compliance.

Since computerization and human-computer interaction (HCI) are the basis of many security breaches and the increased risk of security threats (Abu-Musa, 2006; Loch et al., 1992a), the concept of technostress and ISS requires attention. In this research, we seek to understand the effect of employees' daily IT usage on their security-related behaviors. To fill the research gap, we conducted an empirical study to seek an answer for the following research question: "*Does technostress increase the likelihood of employees' intention to violate ISPs?"* We posit that a combination of technostress creators can put employees in situations where they feel too stressed, anxious, and frustrated to cope with technology. Consequently, perceived stress help them rationalize their non-compliant behaviors to not expend energy and effort on security tasks and in turn, violate ISPs. We also evaluate which aspect of technostress constitutes more effect on user insecure behaviors. Furthermore, our study contributes to the technostress literature by proposing and statistically assessing a new dimension to the second-order technostress construct. In general, the findings of this research illustrates the importance of technostress in the context of ISS, while also provides insights for managers to take account of different types of technostress creators.

2.2 Overview of technostress and research gap

Technostress is a phenomenon introduced by Brod (1984) defining as the perceived stress because of using new IT. Individuals feel different levels of stress, depending on their ability to cope with

new technology like as IT self-efficacy and IT mindfulness and innovativeness (Maier, Laumer, Wirth, & Weitzel, 2019; Tarafdar, Pullins, & Ragu-Nathan, 2015; Yan, Guo, Lee, & Vogel, 2013). The stress arising from IT can be understood through the lens of the person-environment fit model which denotes that stress is a consequence of a misfit between a person and the environment (Ayyagari, Grover, & Purvis, 2011; Cohen, Janicki-Deverts, & Miller, 2007). In other words, an imbalance between human and environment attributes results in stress. According to the person-environment fit theory, people feel stress under two conditions: when the environment does not fulfill a person's expectations and when a person's ability (e.g., skills, time, knowledge) is less than the demands placed by the environment (Edwards, 1996). The former refers to circumstances that the values, needs, and desires of individuals are not fulfilled with resources, supplies, and rewards available in the environment (Edwards, 1996). For example, an employee who likes to receive a promotion but the organization does not provide the opportunity for the achievement. The latter explains inequalities between environmental requirements (e.g., role expectations and organizational norms) and individual capabilities to meet those requirements (Edwards, 1996).

Information system research contextualized this theory to the person-technology fit wherein technology features can cause a person-technology gap by either needs-supplies or demands-abilities misfits (Ayyagari et al., 2011). Technological characteristics such as degrees of usefulness, complexity, reliability, and pace of change compel users to feel they have a low ability to adapt to technology or can create supplies that conflict user values and expectations. Therefore, perceived misfit leads to some levels of stress. For example, low perceived usefulness of technology or unreliable systems (supplies) cannot fulfill users' values and expectations (needs). Factors that induce stress are called stressors, and stressors related to technology are known as technostress creators (Ragu-Nathan et al., 2008; Tarafdar et al., 2010).

Tarafdar et al. (2007b) identified five technostress creators; techno overload, techno-invasion, techno-complexity, techno-uncertainty, techno-insecurity. These are first-order factors of the

technostress construct. They go on to define the constructs. *Techno-overload* occurs when users work more, longer, and faster due to IT use. *Techno-invasion* explains situations where a user's personal and professional lives are blurred due to continuous connectivity to the IT. *Techno-complexity* refers to circumstances in which a user is inexpert to use the IT and needs to spend time and energy to gain knowledge about the IT. *Techno-uncertainty* relates to users who feel uncertain due to the constant change/upgrades of IT. Finally, *Techno-insecurity* describes situations where a user feels he/she may lose his/her job either by computerization of job tasks or having less knowledge about the IT compared to others. All these factors impose a misfit via demands-abilities or supplies–needs and drive IT users to perceive some levels of stress. Technologies that produce extra works have complicated features, or constantly require updates/upgrades, imply high demands exceeding users' ability to simply adopt and execute tasks. Techno-insecurity and techno-invasion could also set up environments that might be incompatible with user expectations and values.

Individuals' responses to perceived stress are known as strain. The strain is defined as the outcome of stress or response (or react) to the stressors (Cooper, Cooper, Dewe, O'Driscoll, & O'Driscoll, 2001; Tarafdar et al., 2010) which can be manifested in forms of psychological reactions or behaviors (Florkowski, 2019; Tarafdar et al., 2010). The response to technostress results in undesirable behavioral and psychological outcomes such as low productivity or task performance, discontinued IT use, and low satisfaction (El Halabieh, Beaudry, & Tamblyn, 2017; Lei & Ngai, 2014; Stich, Tarafdar, Stacey, & Cooper, 2019; Tams, Thatcher, & Grover, 2018).

Technostress has been studied in different contexts such as NeuroIS, social network sites, healthcare, and organizational structure (Maier, Laumer, Weinert, & Weitzel, 2015; Patel, Ryoo, & Kettinger, 2012; Pirkkalainen, Salo, Makkonen, & Tarafdar, 2017; Tams, Hill, de Guinea, Thatcher, & Grover, 2014). However, in the context of ISS, technostress research lacks sufficient understanding, except for some studies that extended the concept of technostress to the domain of

ISS known as ISS-related technostress (Brinton Anderson, Vance, Kirwan, Eargle, & Jenkins, 2016; Chang, Hsu, Li, & Hsu, 2018; D'Arcy et al., 2014; Hwang & Cha, 2018; Singh, Johnston, & Thatcher, 2019), which means that ISS requirements such as security systems and ISPs are the source of stress and consequently lead to employees insecure behaviors or ISP violations. Some research should investigate the direct effect of technostress (due to IT use itself) on employee extra-role behaviors like ISP compliance.

2.3 Research model and hypotheses development

2.3.1 Techno-unreliability: a new dimension of technostress

As described, the five first-order constructs of technostress instrument (techno overload, techno-invasion, techno-complexity, techno-uncertainty, techno-insecurity) have been frequently used in literature. One dimension that seems to be missing is techno-unreliability, which means that due to the complexity of technologies, they are not consistent and reliable (Butler & Gray, 2006; Forester & Morrison, 1990). System breakdowns, software/hardware failure, speed problems (low response time), interrupted Internet connection, and unavailability of online services are common reliability problems (Brinton Anderson et al., 2016; Hudiburg, 1995). Systems unreliability leads to undesirable outcomes such as social vulnerability (Forester & Morrison, 1990), low IT adoption (Wachira & Keengwe, 2011), and most importantly, enhanced stress in users (Ayyagari et al., 2011; Califf, Sarker, & Sarker, 2020; Fischer, Pehböck, & Riedl, 2019). For example, a qualitative study by Fischer et al. (2019) showed that techno-unreliability interrupts task accomplishments, causes work loss (e.g., losing an order via email), and makes users feel angry and unhappy when they experience time pressure and are highly dependent on technology. Califf et al. (2020) reported that unreliability of health information technology (HIT) prevents nurses from executing their primary job like documenting patient data. One example is an intensive care nurse who can’t conduct her mandatory charting of records into the electronic records management (ERM) program because the

system is down and she must sit on the phone waiting for the IT department while at the same time her patients require her attention.

Recently, scholars called for quantitative investigations into the dimensionality of technostress in which the technostress instrument needs to be updated in order to include a new dimension, techno-unreliability (Fischer et al., 2019; Fischer & Riedl, 2015). Thus, we propose techno-unreliability as a new additional first-order construct to the other dimensions and include it in our theoretical model to assess the relationship between technostress and other constructs of the study. Following the person-technology fit model, we argue that unreliable technologies create environments with low resources that do not meet users' needs and expectations. Thus, the misfit can be a source of stress. Despite previous study by Califf et al. (2020) investigated techno-unreliability of HIT reduces performance of performing primary job tasks (intra-role), we argue that techno-unreliability can be a factor that inhibits employees from performing extra-role activities like ISP compliant behaviors as employees usually perceive security tasks are external activities and are not a part of their job (Albrechtsen, 2007; Xu & Guo, 2019). When individuals struggle to accomplish tasks, techno-unreliability can exacerbate the situation thus causing employees to neglect ISPs.

2.3.2 Technostress and perceived strain

Psychological or behavioral response to stressors is defined as *strain* (Sarabadani, Carter, & Compeau, 2018; Tarafdar et al., 2010). The extant stress literature denotes the positive relationship between stressors and strain. Research shows high levels of perceived stressors are highly impactful on users' psychological and emotional reactions (Burke, Brief, & George, 1993; Fisher, Kerr, & Cunningham, 2019; Keenan & Newton, 1985; Kinman & Jones, 2005; Richardson, Yang, Vandenberg, DeJoy, & Wilson, 2008). Regarding technostress creators, research depicts technostress influences individuals' emotions such as work exhaustion, burnout, techno fatigue, techno exhaustion, emotional responses (e.g., deterrence, loss, and achievement emotions), end-

user satisfaction, and job satisfaction (Gaudioso, Turel, & Galimberti, 2017; Ioannou & Papazafeiropoulou, 2017; Sarabadani, Compeau, & Carter, 2020; Turel & Gaudioso, 2018).

We follow the psychological aspect of strain (i.e., the extent to which the user feels tired, drained, or burned out due to IT usage) similar to the study by Ayyagari et al. (2011). Corresponding to the past research on the positive impact of technostress on the perceived strain, we hypothesize that there is a positive relationship between technostress and strain with one difference. We extended the technostress instrument by adding techno-unreliability to the second-order technostress construct, which, to the best of our knowledge, has not been studied in the technostress literature. Therefore, we hypothesize:

H1: Technostress is positively related to perceived strain.

2.3.3 Perceived strain and violations of ISPs

Research has shown that strain influences users behaviors, and it leads to adverse behavioral outcomes such as substance abuse (Osborne, 2019), low academic performance (Cao, Masood, Luqman, & Ali, 2018; Yu, Shi, & Cao, 2019), physical issues and reduced job effectiveness (Wang, Tan, & Li, 2020), lower work performance and productivity (Chen & Karahanna, 2018). There is also evidence that explains strain makes individuals engage in criminal behaviors (Agnew, 1992). According to Singh et al. (2019), employees who are monitored at work perceive high levels of strain and, in turn, are more likely to involve in ISP non-compliance behaviors. Also, previous research found the negative effects of workplace stress and information security complexity, uncertainty, and overload are associated with employees' ISP violations (D'Arcy et al., 2014; D'Arcy & Lowry, 2019; Hwang & Cha, 2018). Hence, we argue that employees with high levels of perceived strain (tiredness and feeling burnout) due to high HCI are more likely to engage in ISP violations for two reasons. First, stressed-out individuals experience cognitive fatigue and exhibit

low performance through the diminished conscious cognitive process (Brinton Anderson et al., 2016; Sellberg & Susi, 2014) and become more likely to commit a misbehavior (e.g., sending information to a wrong recipient, clicking on a phishing link). Second, engagement in extra-role activities requires additional time and effort. Stressed out employees are too exhausted to give priority to security tasks through a cost-benefit analysis of compliance (Bulgurcu et al., 2010). Hence, we hypothesize:

H2: Perceived strain is positively related to the intention to violate ISPs.

2.3.4 Technostress and violations of ISPs

In prior sections, we explained stressors relate to both psychological and behavioral strain (Sarabadani et al., 2018; Tarafdar et al., 2010), and we discussed the relationship between technostress and psychological aspects of strain in Hypotheses 1. Here, we argue that technostress can have an impact on the behavioral aspect of strain in terms of security-related behaviors, in particular, ISP violations. Previous research has extensively examined the inverse relationship between technostress and behavioral outcomes such as performance, productivity, IT usage, perception of health behavior, and job turnover (El Halabieh et al., 2017; Patel et al., 2012; Tams et al., 2018; Tu, Wang, & Shu, 2005). Corresponding to those negative outcomes resulting from technostress, we postulate that technostress can result in ISP violations. This can happen in many ways.

First, users who perceive some levels of complexity with technologies inherently feel incompetent and need to spend more time and energy to learn how to use the technology. Subsequently, they may ignore ISPs in order to solve techno-complexity issues. Second, techno-uncertainty occurs due to the frequent upgrades and use of innovative technologies. Adopting/upgrading new technologies can be frustrating because employees may need to experience a different particular system. The unfamiliarity with the features of new IT and acceptable use policy may threaten ISS. Third, techno-

overload and techno-unreliability indicate users may prioritize primary tasks over ISP activities. While employees use ICTs, it may be perceived as extra work processes. Users may need to perform more tasks, work faster, and receive more information by running multiple applications at the same time, which can enhance the level of stress in users to accomplish tasks. Similarly, unreliable IT causes interruptions and requires users to tackle system problems. Both circumstances cause systems to be vulnerable to ISS threats since the main focus of users is on performing primary tasks. Forth, stress through techno-invasion can be better perceived as employees constantly use ICTs to be reachable. This suggests that they become highly dependent on technology, mainly to use personal devices (PC or phones) in order to respond to emails and conduct required work processes. This can enhance vulnerability to ISS threats as using personal devices for work purposes is recognized as a widespread security threat (Niehaves, Köffer, & Ortbach, 2012), where employees are more likely to ignore ensuring the updated security software on personal devices (e.g., antivirus). Finally, techno-insecurity can reduce employees' intention to comply with ISPs. Due to the high IT dependency, employees may feel stressed and uncertain about keeping their jobs because of either not coping with new evolved applications or being substituted by automatization. Consequently, the instability of the work environment makes employees devote less effort regarding the organizational ISPs.

Based on the above discussion, we hypothesize that technostress influences employees' intention to violate ISPs positively.

H3: Technostress is positively related to the intention to violate ISPs.

The literature follows the stressors-strain-outcome framework to investigate the effect of stress on individuals' behaviors or emotions (Choi, Kim, Lee, & Lee, 2014; Gaudioso et al., 2017; Islam et al., 2018; Yu et al., 2019). According to this framework, perceived strain mediates the relationship between stressors and particular outcomes, meaning that stressors make individuals perceive strain,

which in turn, results in behavioral outcomes. Drawing on this framework, we hypothesize that technostress makes users feel too drained and exhausted about using technology to spend additional time and energy on ISS requirements (i.e., cost-benefit analysis of compliance). As a result, they are more likely to engage in non-secure behaviors and violate ISPs. Thus, we hypothesize:

H4: The influence of technostress on the intention to violate ISPs is mediated by perceived strain.

Figure 2.1 depicts our research model, describing technostress increases employee intention to violate ISPs either directly or through the strain as a mediator.

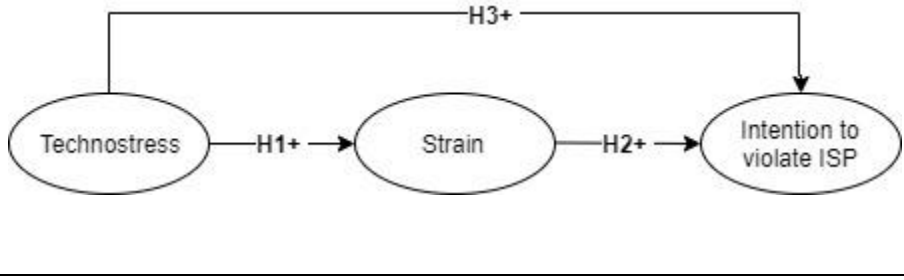

Figure 2.1 Research Model

2.4 Research Method

2.4.1 Sample and measures

We assessed the research model empirically using a sample of employees who had technology-based profession. We used the screening method to ensure our sample of participants perform their job tasks using any types of technologies listed in Table 2.1, such as desktop computers, laptop, tablet, or smart appliances. Data was collected from a crowdsourcing marketing research company located in the United States, which distributes online surveys among participants who are qualified for the study. The marketing research company distributed the survey among their panel members and volunteer employees chose to take the survey. This platform allows for collecting anonymous responses and ensuring a heterogeneous sample, covering organizational differences from a wide range of industries and job positions. After completing the survey, respondents received a small

monetary reward for providing a complete and honest response. Fifty-four responses were eliminated due to incompleteness or failure to answer attention check questions. We obtained 356 responses for our data analysis with diversity in levels of education, age, gender, and technology use (see Table 2.1).

To measure the research model constructs, respondents received a set of questions designed to measure technostress creators and strain (See Appendix, Table 2.A). The technostress construct was measured as a second-order construct reflecting on techno-overload, techno-invasion, techno-complexity, techno-insecurity, and techno-uncertainty, where each construct was measured using validated items adapted from Ragu-Nathan et al. (2008).To measure techno-unreliability, we reviewed the literature to use the concept of technology unreliability (Fischer et al., 2019; Hudiburg, 1995). We closely followed the definition of the construct to develop a four-item scale reflecting system breakdown, system speed, and instability of the Internet. We also added a 3-item tech-reliability scale used in Ayyagari et al. (2011) (although they were removed from the analyses due to the low item validity and reliability). The items for the strain construct were based on Moore (2000). All items were adapted from the well-established scales and our results (discussed in the later section) indicate to the validity and reliability of our selected items.

2.4.2 Scenarios

We used a hypothetical scenario approach to measure the dependent variable of our model, intention to violate ISPs. Scenarios provide subjects with a written description of a real situation and ask respondents for the likelihood of their intention of performing a specific behavior if they were in such a situation (Trevino, 1992). Scenario method offers several advantages for studying undesirable behaviors in terms of indirect measuring of user intention to commit unethical behavior, providing situational details impacting decisions, and measuring behaviors prospectively

Table 2.1 Descriptive Statistics of Survey Respondents (N=356)

Employment Status		Industry		Gender	
Full- time	290 (81.5%)	Education	40 (11.2%)	Male	174 (48.9%)
Part-time	60 (16.9%)	IT Services	108 (30.3%)	Female	182 (51.1%)
Unemployed	6 (1.6 %)	Healthcare	41(11.5%)		
		Government (Non- Profit)	22 (6.2%)		
		Other	145 (40.8%)		
Age			Education		
18-30	78 (22%)		High School or equivalent	78 (21.9%)	
31-40	129 (36.2%)		College graduate (4 years)	205 (57.6%)	
41-50	74 (20.8%)		Masters'/Doctoral Degree	64 (18%)	
51-60	50 (14%)		Other	9 (2.5%)	
61 or older	25 (7%)				
Daily technology Usage at the Workplace			Years of Work Experience		
< 3 hours	24 (6.7 %)		< 2 years	11 (3.1%)	
3-6 hours	136 (38.2%)		2-5 years	46 (13%)	
> 6 hours	196 (55.1%)		5-10 years	65 (18.2%)	
			> 10 years	234 (65.7%)	
Technologies used for work purposes *					
Desktop Computer	281 (79%)		Smart Phone	209 (59%)	
Wearable and smart Appliances	95 (27%)		Laptop computer	35 (9.8%)	
Computer Tablet	191 (54%)		Voice to text devices	12 (4%)	
Facial recognition system	7 (2%)		Other	36 (10%)	

* Note that the sum is not equal to 356 because each person uses more than one device.

with present perceptions (M. T. Siponen & A. Vance, 2010). We adapted five scenarios as common ISP violations, including password sharing, password writes down, failure to log-off, USB copy, and data leakage based on ISS field surveys and previous research (D'Arcy et al., 2014; M. T. Siponen & A. Vance, 2010). Moreover, we conducted interviews with three ISS practitioners (chief information security officer and information security analyst) who suggested another critical security issue: click on links without verification of the source. We developed an original ISP violation scenario describing clicking on unknown links. Ultimately, respondents received one of the six randomly selected scenarios. (See Appendix, Table 2.B). We measured intention to violate ISP using two items adapted from D'Arcy et al. (2014), asking for the likelihood of performing a particular behavior similar to the actor in the scenario. We also asked respondents to rate the realism

of each scenario ranged from 1 (highly unrealistic) to 7 (highly realistic). The average realism score for each scenario was at least 5.35, which ensures scenarios were reasonably realistic.

2.5 Results

We used Mplus as the primary statistical tool to assess the measurement and structural models in our study (Muthén & Muthén, 2016). While there are other good software tools such as AMOS and Stata and each have their strengths, we opted for Mplus as it is a commonly used statistical tool in the field of social sciences with more flexibility to conduct various models with latent variables (Chang, Gardiner, Houang, & Yu, 2020). We conducted a covariance-based method, structural equation modeling (SEM), to analyze constructs and the relationships as it is better suited for model assessment, including second-order constructs (MacKenzie, Podsakoff, & Jarvis, 2005).

2.5.1 Measurement model

We conducted various tests to validate the psychometric properties of the measurement model based on model fit, composite reliability, convergent, and discriminant validity of the constructs (D. Barclay, C. Higgins, & R. Thompson, 1995). First, following a two-stage approach to testing the secondo-order construct (Becker, Klein, & Wetzels, 2012), we conducted a confirmatory factor analysis (CFA) on the entire set of items where each observed variable restricted to load on its first order construct. Then, we ran a CFA for a model considering second-order technostress construct with and without techno-unreliability construct to verify techno- unreliability as a new dimension (Table 2.2).

Table 02.2 Goodness of Fit for the Measurement and structural model

Goodness of fit measures	χ^2 (d.f.)	CFI	RMSEA	SRMR
Good model fit ranges	Non-sign.	> 0.90	< 0.1	< 0.1
CFA model (first-order constructs)	863.63 (377)	0.93	0.06	0.056
CFA model (second-order TSC without techno-unreliability)	837.05 (291)	0.91	0.073	0.08
CFA model (second-order TS including techno-unreliability)	1042.55 (396)	0.91	0.068	0.08

TSC, technostress construct

First, we performed a chi-square difference test to compare two models. The results showed two models are significantly different ($\Delta\chi^2$ (105) = 205, P < 0.001) with an improvement in fit index (RMSEA). Second, results of R-square determined the variance of the first order factor explained by the second order factor construct wherein techno-unreliability accounts for 6% variance of technostress construct. Furthermore, according to MacKenzie, Podsakoff, and Podsakoff (2011), we computed the sum of the squared loadings of the primary factors on the second order technostress construct. The overall variance of 2.37 with the five factors (techno-overload=0.76, techno- invasion= 0.92, techno- complexity= 0.59, techno- insecurity= 0.71, and techno-uncertainty= 0.31) increased to 2.76 with six factors including techno-unreliability (techno-overload=0.64, techno- invasion= 0.75, techno- complexity= 0.85, techno- insecurity= 0.98, and techno-uncertainty= 0.15, and techno-unreliability= 0.25). This suggests that the overall variance for the technostress construct improved by approximately 16.2% with the inclusion of techno-unreliability. Third, according to the results of Table 2.2, the second-order factor model including techno-unreliability compared to the first-order factor model has more degrees of freedom and fewer parameters to be estimated. This suggests that the second-order factor model with techno-unreliability should be accepted as it is a more parsimonious model (Grover, Teng, & Fiedler, 2002; Wright, Campbell, Thatcher, & Roberts, 2012). Finally, loading of techno-unreliability along with other second-order factor loadings were highly significant (see Figure 2.2), providing support for the second-order model with techno-unreliability (Tippins & Sohi, 2003). Thus, techno-unreliability is confirmed to be a new reflective construct to the second-order technostress construct. Overall, the results of fit indices reported in Table 2.2 (CFI, RMSEA, SRMR) suggested that the data fit the models well based on the recommended fit measures for CFI > 0.90, RMSEA < 0.10, and SRMR < 0.10 (Hair, Black, Babin, Anderson, & Tatham, 1998; Kline, 2015).

To ensure indicator reliability, we checked items' loading in which all showed high-factor loadings above the recommended minimum value of 0.60, indicating each latent variable accounts for at

Table 2.3 Confirmatory Factor Analysis of Statistics

Standardized latent constructs loadings

Latent variable	Item	TO α=0.86	TI α=0.81	TC α=0.84	TS α=0.83	TU α=0.87	TR α=0.87	S α=0.95	INT α=0.93	R^2
TO	TO1	0.80								0.64
	TO2	0.81								0.65
	TO3	0.78								0.61
	TO4	0.61								0.38
	TO5	0.75								0.56
TI	TI1		0.71							0.51
	TI2		0.65							0.43
	TI3		0.83							0.49
	TI4		0.70							
TC	TC1			0.82						0.67
	TC3			0.67						0.45
	TC4			0.73						0.54
	TC5			0.82						0.67
TS	TS1				0.80					0.64
	TS3				0.78					0.61
	TS4				0.66					0.44
	TS5				0.69					0.47
TU	TU1					0.80				0.64
	TU2					0.86				0.73
	TU3					0.85				0.73
TR	TR1						0.67			0.45
	TR2						0.78			0.60
	TR3						0.87			0.76
	TR4						0.84			0.70
S	Strn1							0.93		0.87
	Strn2							0.94		0.88
	Strn3							0.88		0.76
	Strn4							0.88		0.77
INT	Int1								0.96	0.92
	Int2								0.91	0.83

TO, techno-overload; TI, techno-invasion; TC, techno-complexity; TS, techno-insecurity; TU, techno-uncertainty; TR, techno-unreliability; S, strain; INT, intention to violate ISP; α, Cronbach's alpha

least 50% of the variance of the underlying construct (Chin, 1998). To examine construct reliability, we calculated the average variance explained (AVE), composite reliability (CR), and Cronbach's alpha (α) reliability for each construct which all fulfilled based on the recommended values of 0.50

for AVE and 0.70 for CR and α (Chin, 1998; Gefen, Straub, & Boudreau, 2000). Furthermore, the discriminant validity of each construct was verified by comparing the square root of the AVE to the inter-construct correlation coefficients (see Table 2.3 & 2.4) (Fornell & Larcker, 1981b). We also note that the means scores depicted in Table 2.4 provide some indication that all of the techno-stressors are of concern to our respondents with techno-uncertainty and techno-unreliability being their greatest concerns. Techno-complexity and techno-insecurity were not as concerning as the other stressors while strain appeared to be only of slight concern for them.

Finally, we conducted Harman's one-factor test to analyze the effect of common method variance (CMV) (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003), where the sign for CMV is the emergence of a single factor accounting for the majority of the variance. The result showed that 27.46% of the variance in all variables was explained by a single factor (less than 50%). Furthermore, following Paul A. Pavlou, Huigang Liang, and Yajiong Xue (2007), a correlation matrix between constructs did not show a high correlation among constructs ($r^2 > 0.90$). This provides additional support that CMV is not an issue in our study.

Table 2.4 latent variable statistics

		Mean	Std. Dev.	CR	AVE	1	2	3	4	5	6	7	8
1	TO	3.77	1.77	0.87	0.57	**0.76**							
2	TI	3.27	1.84	0.82	0.53	0.69	**0.73**						
3	TC	2.65	1.6	0.85	0.59	0.46	0.57	**0.77**					
4	TS	2.64	1.6	0.82	0.54	0.58	0.70	0.87	**0.73**				
5	TU	5.1	1.41	0.88	0.70	0.33	0.30	-0.05[#]	0.09[#]	**0.84**			
6	TR	4.6	1.78	0.87	0.63	0.34	0.28	0.17	0.18	0.31	**0.79**		
7	S	2.9	1.75	0.95	0.82	0.57	0.51	0.69	0.72	0.06[#]	0.27	**0.90**	
8	INT	2.58	1.9	0.93	0.88	0.04[#]	0.17	0.28	0.22	-0.12	-0.002	0.15	**0.94**

[#] P>0.1, The diagonal entries are the square root of AVE.
TO, techno-overload; TI, techno-invasion; TC, techno-complexity; TS, techno-insecurity; TU, techno-uncertainty; TR, techno-unreliability; S, strain; INT, intention to violate ISP; CR, composite reliability; AVE, average variance explained.

2.5.2 Structural model

Next, we used SEM to test the hypothesized model. We modeled the six sub-dimensions into a second-order construct, technostress and related to the other constructs. Table 2.5 presents the fit indices and standardized path coefficients for the hypothesized relationships. According to Byrne (2013), with a good model fit and meaningful path coefficients, the structural model can be assessed by adding a new path as long as the chi-square difference test provides significant statistics, implying the second model with one added path is different and meaningful than the previous model. Taking this approach, in the first model, we examined the relationship between technostress and strain (Model 1). All fit measures indicated a good fit, and the significant path coefficient suggested that Technostress is positively related to strain. (β= 0.77, P <0.001). Thus, H1 is supported. To examine H2, we added strain and intention to the violate ISPs relationship. Because each participant received a random scenario, to test the effect of strain on the intention to ISP violation, we controlled for

the effect of scenario type. The reason was based on the results of a one-way ANOVA test where we found the level of intention significantly depends on the type of the scenario (reported intention to the sharing password scenario had the highest average of 3.42, followed by a click on links with the minimum average at 2.31). We also controlled for realism as we found the perception of scenario realism is significantly related to intention. Model 2 exhibited a good model fit and the chi-square difference test with Model 1 was significant ($\Delta\chi^2$ (58) = 131, P < 0.001). The positive path coefficient (β= 0.18, P <0.001) of the strain and intention to violate ISP relationship provided support for the H2.

Finally, in a combined model, we examined the relationship between technostress and intention to violate ISP (model 3). Model 3 exhibited a reasonable fit and significantly differed from model 2 ($\Delta\chi^2$ (1) = 12, P < 0.001). The positive, direct relationship between technostress and intention to

violate ISPs (β= 0.34, P <0.001) provided support for H3. However, the relationship between strain and intention to violate ISP is not significant (β= -0.08, P>0.05). As such, the mediation effect was not observed based on Baron and Kenny (1986). Also, we conducted a Sobel test for the indirect effect of technostress on ISP violation intention through strain using Preacher's online Sobel test calculator (http://quantpsy.org/sobel/sobel.htm). The Sobel test statistics were not significant (Z= -0.88, p > 0.05). and H4 is not supported.

Figure 2.2 depicts standardized path coefficients, significance levels, and a statistical measure of R^2- coefficient of determination of the combined model. Given the minimum 10% criterion for the R^2 value of a dependent variable to make meaningful interpretation (Falk & Miller, 1992), our theoretical model demonstrated sufficient explanatory power (R^2= 0.14).

Table 02.5 Standardized Path Coefficients and Fit Indices for the Structural Models

Model fit statistics			
	Model 1	Model 2	Model 3
χ^2 /df	1043.47 (397)	1174.45 (455)	1162.91 (454)
CFI	0.91	0.90	0.90
RMSEA	0.068	0.067	0.066
SRMR	0.085	0.085	0.086
Standardized Path coefficients			
TSC→ TO	0.66***	0.67***	0.66***
TSC→ TI	0.74***	0.74***	0.73***
TSC→ TC	0.87***	0.86***	0.87***
TSC→ TS	0.96***	0.96***	0.96***
TSC→ TU	0.13*	0.14*	0.13*
TSC→ TR	0.27***	0.27***	0.26***
TSC → Strain	0.77***	0.77***	0.77***
Strain → INT		0.18***	-0.08
Scenario→ INT		0.12*	-0.11*
Realism → INT		0.21***	0.22**
TSC → INT			0.34***
Hypotheses Test	H1 was supported	H2 was supported	H3 was supported H4 was not supported

TO, techno-overload; TI, techno-invasion; TC, techno-complexity; TS, techno-insecurity; TU, techno-uncertainty; TR, techno-unreliability; S, strain; INT, intention to violate ISP; TSC, technostress construct; *p <0.05; ** p<0.01; *** p <0.001

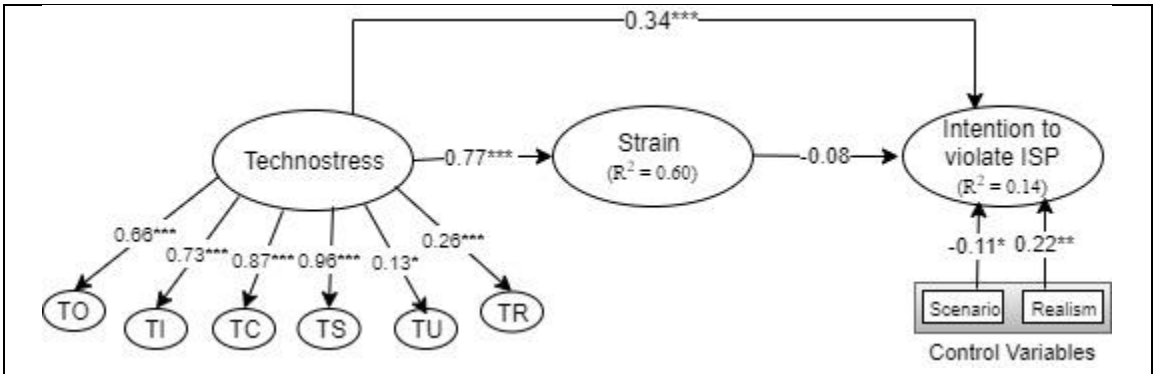

Figure 2. 2 Research Model Showing Results of SEM analysis

*p <0.05; ** p<0.01; *** p <0.001

2.5.3 Post hoc analysis

Our post hoc analysis focuses on the direct effect of each factor of technostress on intention to ISP violations. Initially, we treated technostress as a combination of six stressors and studied its effect on users' behavioral intentions. However, each of the techno-stressors might exhibit different impacts which suggests some more influential to users' insecure behaviors than others. Therefore, we decomposed the relationship between technostress and intention to violate ISPs into six separate relationships. We regressed ISP violation intention on each stressor independently to address the multicollinearity problem which appears when multiple constructs are used to predict one variable (Grewal, Cote, & Baumgartner, 2004; Kaplan, 1994). The standardized path coefficients for all stressors were significant except for techno-overload and techno-unreliability (See Figure 2.3). We interpret the results to emphasize on the role of techno-complexity, techno-insecurity, and techno-invasion in enhancing employee intention to violate ISPs. Surprisingly, the effect of techno-uncertainty on ISP violation intention is negative. One can infer that a user with perceptions of uncertainty and ambiguity in technology is more likely to be aware of security risks and may take precautions regarding information security practices. Techno-overload and techno-unreliability did not influence user intention to violate ISPs. Nonetheless, the effect of techno-overload became significant (β= 0.13, P< 0.05) when techno-unreliability presented in the model. This suggests the

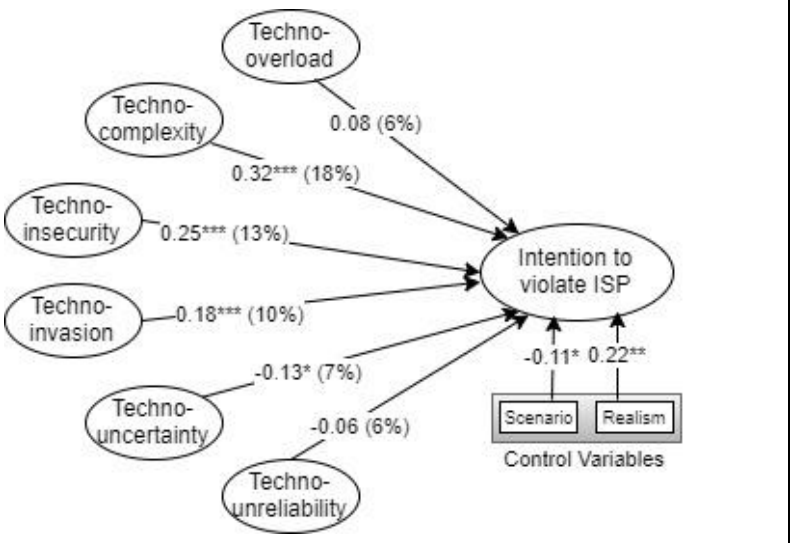

Figure 2.3 Results of post hoc analysis, standardized path coefficient (R^2)

*p <0.05; ** p<0.01; *** p <0.001

presence of an indirect effect or a causal confounder since techno-unreliability causes techno-overload (β= 0.34, P< 0.001). One interpretation is that techno-unreliability leads to perceptions of greater techno-overload which in turn contributes to higher ISP violations.

2.6 Discussion and contributions

Although the value of IT is very apparent for organization performance, due to the dual nature of IT, overuse of technology and ICTs may give rise to unintended consequences like technostress. This study attempted to understand technostress's impact on organizational information security. Technostress is a phenomenon that influences employees' ISS-related behaviors. We demonstrated that users who perceive high levels of technostress are more likely to violate ISPs and threaten organizations' information security. More specifically, our results make several contributions to the literature.

First, previous technostress literature treated technostress as a second-order construct consisted of five stressors: techno-overload, techno-complexity, techno-uncertainty, techno- invasion, and techno-insecurity (Ragu-Nathan et al., 2008; Tarafdar et al., 2007b). Recently, scholars called for the addition of a new dimension, techno-unreliability to the technostress instrument (Califf et al., 2020; Fischer et al., 2019). In this research, we extended the dimensionality of the technostress instrument to six factors by including techno-unreliability as a new stressor and confirmed its psychometric properties. While existing five stressors successfully determine some level of technostress, we posited that techno-unreliability should be considered as an additional techno-stressor. Furthermore, we assessed the relationship between technostress (including new dimension) and its psychological outcome-strain. We provided additional support to the past research for the positive impact of technostress on strain with highlighting the role of techno-unreliability in enhancing perceived strain. In fact, we demonstrated a combination of six techno-stressors causes users incur to exhaustion and burnout due to considerable IT use.

Second, we extended technostress literature to the context of ISS. Previous literature on ISS explored the effect of security-related stressors on users' ISP compliance behaviors (D'Arcy et al., 2014; Ho-Jin & Cho, 2016). They specifically examined three stressors: overload, uncertainty, and complexity. However, we filled the gap and generalized security-related stressors to the concept of technostress, where technostress includes using any type of technology. We found it is not only ISS requirements (ISPs and security systems) that act as stressors to make users engage in insecure behaviors. In reality, as we hypothesized, features of ICTs and other information systems create situations where employees perceive high levels of techno-overload, techno-insecurity, techno-complexity, techno-uncertainty, techno-unreliability, and techno-invasion. A combination of these stressors provides a favorable environment for employees to pay less attention to their extra role tasks (ISS requirements) and violate ISPs. Simply put, technostress does lead to intention to violate ISPs. This finding emphasizes on the importance of technostress on user behaviors. While past

research depicted the negative impact of technostress on user productivity and performance (Tams et al., 2018; Tarafdar et al., 2007b), we contributed further by examining its influence on user security-related behaviors.

Third, previous contributions from stress and IS revealed that strain leads to criminal behaviors and adverse outcomes (Agnew, 1992; Singh et al., 2019). We extended the concept of strain to the context of ISS. We found employees who perceive high exhaustion and drained are often non-compliant with ISPs and have higher intentions to violate ISPs. This might happen through either diminished mental process for a cognitive fatigue user or prioritization of primary tasks to the ISS requirements. However, strain loses its impact once technostress presents. Contrary to the research by Gaudioso et al. (2017) and Islam et al. (2018), our results of mediation analysis showed strain does not mediate the relationship between technostress and an outcome- intention to violate ISPs, suggesting that it is not the perception of exhaustion and burnout (of IT use) that make users violate ISPs. Instead, technostress itself is strong enough to impact users' intention to not comply with ISPs directly. Each of the six techno-stressors creates situations for ISP non-compliant behaviors, which increase system vulnerabilities to ISS threats. Thus, a more parsimonious model may be sufficient to study the effects of techno-stress on the intention to violate ISPs.

Forth, in addition to being consistent with past research that treats technostress as a second-order factor on user behavior (Ragu-Nathan et al., 2008; Tarafdar et al., 2007b), we took a new approach and decomposed the technostress construct to its six sub-dimensions to understand which techno-stressors act stronger in influencing users' security-related behavior. The results of our post hoc analysis revealed that techno-complexity, techno-invasion, techno-insecurity, incline users to be more engaged in non-compliant behaviors with ISPs. Among these factors, techno complexity appears to have the highest negative impact on user ISP compliance. The more the system is complex, the less a user follows good security practices since s/he may be involved to solve complicated features of a system rather than following ISP requirements. Techno-insecurity implies

an employee perceives some levels of instability at the workplace. Hence, it may result in low organizational commitment which in turn reduces intention to perform best ISS practices (Hwang & Cha, 2018). Techno-invasion suggests that a user is already exhausted enough of not being free of technology; then may pay less attentions to ISS requirements where s/he is required to be responsive anytime. Finally, our findings indicated that techno-overload only at the presence of techno-unreliability can lead to ISP violations. In other words, techno-unreliability adds to techno-overload perceived by users. This is consistent with prior findings by Ayyagari et al. (2011), who found the more technology reliability, the less the perceived work overload. We surmise that additional tasks levied on the user by techno-unreliability (i.e. having to call the help desk, finding workarounds) simply adds to the overload. Therefore, prioritization of primary tasks can justify why users are less likely to spend additional time and effort in order to comply with ISPs.

For practitioners, the implication is that excessive use of IT might be threaten to organizational ISS. Organization leadership and IT departments should consider the dimensions of technostress as they levy work requirements on their employees and be aware that too much stress and strain will result in ISS vulnerabilities. For example, they should consider reducing the required amount of ICT usage like e-mail loads as it might increase the probability of accidental clicks on phishing links like using a filtering mechanism to limit the number of received emails. Information security professionals should also consider providing immediate IT technical support to address the additional techno-stressor (techno-unreliability) brought on by the additional workload. Techno-unreliability may result in employees finding unsecure work-arounds to accomplish their required duties at the expense of ISP. The findings would guide practitioners and ISS professions to focus on certain IT features to alleviate the negative impacts.

2.7 Limitations and future research

We acknowledge the findings of this study are restricted by some limitations. First, although we took the scenario approach to manipulate users' security-related behaviors, the scale measured the employee's intention for information security. Users' actual ISS performance might not be well predicted by reported behavioral intentions. Similar to D. Biros, M. Daly, and G. Gunsch (2004), future research should consider designing experiments to verify the effect of technostress on actual behaviors. Second, techno-uncertainty and techno-unreliability compared to other stressors, showed lower loading reflected on technostress. The findings are similar to previous studies (Ragu-Nathan et al., 2008; Tarafdar et al., 2007b) in which techno-uncertainty had a lower than 40% weight on technostress construct. To assess further, we regressed technostress on techno-uncertainty and techno-unreliability as only two first-order factors. Interestingly, the loading was around 60% with considerable R^2 (> 30%), suggesting that techno-unreliability and techno-uncertainty explained significant variance of second-order technostress construct. However, future research might investigate reflected items that capture these two factors in order to assess their low loading at the presence of other technostress creators.

Third, while we did not control for individual differences such as age, gender, personality traits, or self-efficacy, previous studies found that individual differences determine different levels of technostress perception (Maier et al., 2019; Tams et al., 2018). Our post hoc analyses of regressing demographic factors on technostress, and behavioral intention demonstrated the regression coefficient for job experience and industry sectors are significant. Users with more job experience perceived low levels of technostress and are less engaged in ISP violations. Moreover, depending on the industry, employees realize technostress in different ways. Therefore, future research should investigate a sample of sector-specific data to provide empirical findings for our theorized relationships. We did not observe the statistically significant impact of age and gender on technostress. This is not surprising since a few previous studies could not report that technostress is impacted by these factors (Marchiori, Mainardes, & Rodrigues, 2019; Wang, Shu, & Tu, 2008).

Nevertheless, there is some evidence report older people and women experience high techno-complexity and techno-uncertainty (Marchiori et al., 2019; Ragu-Nathan et al., 2008). Moreover, ISS literature identifies gender as a factor influencing users' intention to comply with ISPs (Herath & Rao, 2009; Ifinedo, 2014). Hence future research should apply gender theories or conduct qualitative approach to provide in-depth insight on the effect of age, gender, and other demographics on the technostress and security-related behaviors.

Finally, it is worthy of investigating the possible mitigating factors of technostress to enhance ISP compliance. Such studies might utilize protection-motivation theory and apply technostress inhibitors (Ragu-Nathan et al., 2008; Vance, Siponen, & Pahnila, 2012) to assess the effects of organizational support (e.g., technical support) and perceived benefits (e.g., promotion or reward expectancy) that might incentivize employees to tackle technostress in favor of complying with ISPs.

2.8 Conclusion

This study investigated how employees respond to perceived technostress in terms of ISP violations. Beyond the specific security-related stressors, we extended the technostress phenomenon to the behavioral research domain of ISS, which has not been addressed in previous research. Moreover, we empirically evaluated and added a new dimension to the technostress instrument called "techno-unreliability." Our findings indicated that a set of techno-stressors (complexity, uncertainty, insecurity, workload, unreliability, invasion) compels users to become involved in insecure behaviors. Also, users with high levels of perceived strain (burnout) due to IT use are more likely to violate ISPs. Furthermore, an in-depth investigation on each sub-dimension of technostress led to a better understanding of the effect of each techno-stressors on employee behavior where some stressors had greater impact on rising the likelihood of ISP non-complaint behaviors. Overall, our findings provided insights into the negative consequences of IT on users'

security- related behaviors. Such insights can help researchers to assess individual differences in technostress perceptions and various features of technology in order to propose mitigation strategies to alleviate unintended outcomes of IT usage.

CHAPTER III

UNDERSTANDING EMPLOYEE INFORMATION SECURITY POLICY COMPLIANCE FROM ROLE THEORY PERSPECTIVE

3.1 Introduction

The number of information security (InfoSec) breaches has been rising recently(IBM, 2019), and InfoSec professionals report employees as the main InfoSec threat in protecting organizational assets(Crossler et al., 2013). Organizations implement InfoSec policies (ISPs) and require employees to follow security guidelines, but not all comply(Cheng, Li, Li, Holm, & Zhai, 2013). In most cases, employees violate ISPs without malicious intentions as they confront situations at the workplace that make them neutralize and rationalize their security inactions(Bulgurcu et al., 2010; M. T. Siponen & A. Vance, 2010). Information system (IS) research identified a situation wherein the perception of stress results in poor behavioral outcomes at the workplace(Ayyagari et al., 2011; Guimaraes & Igbaria, 1992; Ragu-Nathan et al., 2008; Tarafdar et al., 2007b). Stress is a consequence of disparity between environmental demands and individuals' ability to respond to required demands(Lazarus, 1993). While researchers acknowledge the adoption of security system technologies and enforcement of ISPs are necessary, they can create a stressful environment for users to promote ISP violations(D'Arcy et al., 2014; D'Arcy & Teh, 2019; Pham, El-Den, & Richardson, 2016). Scholars conceptualize this phenomenon as security-related stressors of technostress (i.e., stress related to technology use(Tarafdar et al., 2007b)). Security requirements involve additional levels of complexity, uncertainty, and workload (security-related

techno-stressors), making employees spend additional time and effort to learn and understand complicated and continually updated technological aspects of security. Due to the cost associated with ISP compliance, users rationalize their behaviors to violate ISPs. As an exemplar study, D'Arcy et al. (2014) investigated the effect of security-related stressors on employee intention to violate ISP. They drew on emotion-based coping theory and moral disengagement theory as mechanisms to explain how individuals respond to security-related stressors through moral justification, detaching from reality, and minimizing the consequences of behaviors. One area of research that appears to require additional investigation is role stress at the workplace.

In addition to technology use as a source of stress in the workplace(Ayyagari et al., 2011), role-stressors are considered as work-stressors too(Chen & Spector, 1992; Henle & Blanchard, 2008; Kahn, Wolfe, Quinn, Snoek, & Rosenthal, 1964). According to the organizational role theory(Biddle, 1986; Kahn et al., 1964), employees perform certain roles for a given job position based on the required expectations. Role theory posits that individual performance (role behaviors) at the workplace depends on the perceived expectations required by official (or unofficial) groups in organizations. Under some circumstances, the roles trigger stress when expectations are too much to handle, are ambiguously defined, or are contradictory to each other(Katz & Kahn, 1978). Past organizational studies demonstrated that role-stressors, including role-ambiguity, role-overload, and role-conflict, reduce job performance, satisfaction, productivity and cause frustration and depression (Beehr, Jex, Stacy, & Murray, 2000; Lambert, Hogan, Paoline, & Clarke, 2005). IS literature contributed to the effect of role-stressors on employee performance, such as job productivity, turnover, strain, organizational commitment, and discontinuance usage(Galluch, Grover, & Thatcher, 2015; Igbaria & Siegel, 1992; King & Sethi, 1997; Tarafdar et al., 2007b; Zhang, Zhao, Lu, & Yang, 2016). With respect to ISP compliance, Hwang and Cha (2018) examined the mediation effect of security-related role-stressors consisted of role-ambiguity and role-conflict on the relationship between security-related techno-stressors and organizational

commitment. They showed security-related techno stressors lead to higher security-related role-stressors, which result in lower organizational commitment. However, they did not investigate how security-related role-stressors, either directly or through organizational commitment, could contribute to security-related behaviors. In their study, D'Arcy and Teh (2019) employed discrete emotions and coping responses as techniques to explain employee ISP compliance as a response to security-related stressors (which they called hindrance stress). Although this study conceptually indicates that hindrance stress may originate due to the role-ambiguity and role-conflict, the authors do not discern multiple dimensions of role stress and do not empirically measure and examine the effect of each role-stressors (e.g., role-ambiguity, role-conflict, and role-overload).

Despite the research on security-related stressors(D'Arcy et al., 2014; D'Arcy & Teh, 2019; Pham et al., 2016) and the noteworthy studies by D'Arcy and Teh (2019) and Hwang and Cha (2018), the effect of stress rooted in employees' role activities, including primary job duties (intra-roles) and security requirements (extra-roles) on their security-related behaviors requires investigation. Our understanding is limited regarding how role stress due to conflict, multitasking, and vague responsibilities influence employees' security-related behaviors. While the popular press often notes that InfoSec is everyone's business, it may not ring true when conflicting roles come into play. When primary job roles are at odds with security roles or when additional duties are levied on employees, this leads to role-stressors that become apparent when employees are forced to choose between the two.

ISPs are usually mandated in organizations, but employees often perceive them as extra-role activities and do not regard them as a part of their job and responsibility(Posey, Roberts, Lowry, & Hightower, 2014). We view employees' primary duties as intra-role tasks and other additional duties that are not in their job description as extra-role duties. There is considerable research investigating intra-role and extra-role duties that aligns with this view(Kim & Mauborgne, 1996; Vigoda-Gadot, 2007). While some studies view the requirements of organizational policies,

including ISPs as intra-role(Hsu, Shih, Hung, & Lowry, 2015), we see them additional duties outside the primary roles of the employees (e.g., a doctor's primary focus is on healing patients, not InfoSec). A deeper discussion of this situation is outside the scope of this research, but we note that in this study, we refer to role-expectations as a combination of intra and extra role-activities (all duties that are officially/unofficially expected to be executed).

In this study, we investigate the impact of perceived role expectations on employee ISP compliance. We aim to extend past research on the role stress in order to explain to what extent different types of role-stressors contribute to ISP compliance behaviors, which then could lead to appropriate mitigating strategies. Particularly, we seek to address the following research questions:

RQ1. How does role stress relate to employee intention to comply with ISP, either directly or through organizational commitment?

RQ2. How does and to what extent each type of role stress impact employee ISP compliance intention?

Although past research has employed coping, neutralization, and social exchange perspectives as theoretical frameworks to explain *why* individuals rationalize their behaviors through emotions and cost-benefit analysis to respond to stress(D'Arcy et al., 2014; Teh, Ahmed, & D'Arcy, 2015), we draw on the role theory to understand *how* the stress induced by overload, ambiguous and conflicting role expectations influence employee ISP compliant behaviors. This research develops and empirically assesses a model to provide knowledge of the effect of three types of role-stressors (conflict, ambiguity, and overload) on employees' intention to ISP compliant behaviors. We argue that while employees perform multiple unclear tasks with conflicting requirements, their perception of stress offsets their actions by focusing on their primary job tasks rather than practicing the best security behaviors. Simply put, when faced with the choice of accomplishing their primary duties or adhering to ISP, the latter will lose to the former. Consistent with Hwang and Cha (2018) we

also investigate the influence of organizational commitment, but here we examine how it mediates the relationship between role stress and ISP compliance intention. Furthermore, as a mitigation strategy to harness role-stressors, we evaluate whether organizational support could moderate role stress to enhance ISP compliance intention. The findings of this study illustrates the significance of role theory in InfoSec context, while also provide guidance for managers to take account of different types of role-stressors.

3.2 Theoretical development

3.2.1 Role theory

Role theory explores human behaviors in a social setting wherein individuals are actors who perform a set of roles within an environment(Biddle, 1986). Individuals perform roles consisted of patterned and expected behaviors based on self-conception or prescribed by others(Wehner & Thies, 2014). Biddle (1986) designated that role theory relates to three concepts: characteristic (pattered) behaviors, social potions, and expectations (scripts). Depending on a given social situation and expectations prescribed for a role, different perspectives have been appeared to describe role theory. He discussed five such perspectives.

- *Functional role theory* concerns a stable social system in which actors with identified social positions perform roles according to the exact taught and prescribed normative expectations. This perspective has become less relevant since social systems are not stable, and social actors may not perform paralleled to expected norms (personal beliefs and cognitions may interfere).

- *Symbolic interactionist role theory* focuses on roles through social interactions where roles are shaped based on a situation perceived by individuals and involves norms, personal beliefs, attitudes, and environmental demands. This perspective fails to address the

boundaries of expectations, how they should be defined, and to what extent personal perceptions can intervene with roles.

- *Structural role theory concerns* structuralism wherein roles are shaped within socially structured relationships reflected by the social environment, not by individuals.

- *Cognitive role theory* concerns behaviors reflected by expectations resulting from a person's own beliefs and others. In other words, performed roles are the outcomes of thought processes that are influenced by perceptions, cognition, and behaviors of self and others.

- *Organizational role theory* describes roles in formal organizations that are task-oriented. Each individual has an identified social position that performs roles according to the organization's required demands as well as norms reflected by other informal groups.

The majority of the role theory research utilizes the organizational perspective of the role theory (Biddle, 1986; Sluss, Van Dick, & Thompson, 2011). The goal is to study how organizational roles influence employee attitudes and performance behaviors in the workplace. An employee in an organization is attached to a position that enacts certain roles corresponded to the normative expectations. The expectations are the combinations of the assigned formal tasks (e.g., intra-role tasks as per job description) and the requirements by others in the organizations (Biddle, 1986; Katz & Kahn, 1978) (e.g., ISP requirements asked by security management). Due to the multiple sources for norms and various perceptions of norms by individuals (Biddle, 1986), employees may not cope with the expectations effectively. For example, role expectations may be interpreted differently from what they are stated by agents (Katz & Kahn, 1978). Also, role expectations may not be defined explicitly, and a person may conduct multiple roles with various expectations that exceed his/her capabilities to manage. These circumstances give rise to the concepts of role-ambiguity, role-conflict, and role-overload. *Role-ambiguity* is the extent to which

a person is not certain about the expectations, while *role-conflict* appears when there are multiple demands with different objectives (Katz & Kahn, 1978). *Role-overload* describes situations when the expectations are more than a person's capabilities to carry out (Kahn et al., 1964). Organizational studies refer to them as role stress constructs that negatively influence human behaviors (Beehr et al., 2000; Lambert et al., 2005). In the next section, we discuss how each of these concepts relates to employee security-related behaviors.

3.2.2 Role stress and ISP compliant behaviors

Role theory(Kahn et al., 1964; Katz & Kahn, 1978) posits that individuals expect to perform according to their defined roles. It also suggests that inconsistency, the tension in task requirements, and uninformed responsibilities cause stress and prohibit them from executing their roles successfully(Kahn et al., 1964). Role stress occurs under three circumstances: role-overload, role-ambiguity, and role- conflict.

Role-overload is defined as a person's perception of not being capable of handling all assigned tasks(Kahn et al., 1964). It happens when role expectations are high, and employees are incapable of addressing all demanding requirements. ISP levies additional duties and tasks on employees. This can be as little as a requirement to lock a computer while walking down the hall to retrieve a print job or a much as having to complete an hour-long security awareness and training program. Either way, the additional tasks eat up valuable time adding to the employees' feelings of stress.

Role-ambiguity describes a lack of clarity in role requirements wherein either an individual does not have adequate knowledge about the task, or the consequence of their performance is unpredictable(Kahn et al., 1964). For instance, telling employees to secure their data when they are not working with it could have multiple meanings. First, it could mean to put it away to prevent unauthorized individuals from viewing it. Second, it could mean locking their computers when

stepping away. Third, it could mean actually encrypting data at rest. This can lead to confusion thereby taking up more of the employees' valuable time.

Role-conflict refers to inconsistent and incompatible task requirements. It happens when there are contradictory responsibilities in which tasks are not well-matched and in harmony with each other(Guimaraes & Igbaria, 1992; Katz & Kahn, 1978). For example, a nurse is required to respond immediately to a 'code blue' (e.g., cardiac arrest) s/he is compelled to respond immediately to save the patient's life. At the same time, ISP requires the nurse to secure her/his computer before leaving the area. These are incompatible tasks. One requires the nurse to not waste a second responding to the code, whereas the other requires her/him to take time to secure their workstation.

At the presence of role-stressors at the workplace, stressed-out people exhibit lower performance as stress diminishes ones' ability to work effectively(Tarafdar et al., 2007b). Past research provided insights into the dysfunctional results of role stress leading to criminal and abusive behaviors such as theft and substance use(Chen & Spector, 1992). It also distracts employees from concentrating on their primary tasks and contribute to cyber-loafing(Henle & Blanchard, 2008).

Behavioral InfoSec literature denotes that when employees experience low job stress, they show better performance in terms of InfoSec awareness (McCormac et al., 2018). Furthermore, a stressful environment at the workplace increases human security errors due to limited functionality of working memory (Renaud & Privacy, 2011) and reduces coping responses to InfoSec requirements (Božić, 2012). ISPs contribute to stress, and employees' perceptions of security-related stressors contribute to the neutralization of ISP violations (D'Arcy & Teh, 2019; Teh et al., 2015). These studies suggest that security requirements cause work impediments (i.e., stress) as the constant change of ISPs is associated with confusion and ambiguity, where one can experience a lack of explicit knowledge and understanding regarding InfoSec (Hwang & Cha, 2018).

We argue that it is not only security-related stressors that lead to insecure behaviors. In fact, under role stress due to conflict, ambiguity, and overload expectations, it is highly probable that employees ignore the best security practices (extra-role duties) in favor of completing primary job responsibilities (intra-role duties). The reason is that they struggle enough with performing multiple, unclear, and contradictory role tasks and refuse to spend additional time and effort to perform security behaviors. As one endeavors to figure out how to accomplish his/her own job requirements, following ISPs are the less prioritized actions to perform. In other words, employees rationalize their ISP violations by focusing on their own job goals and accomplishing their primary tasks effectively. Consequently, they neglect and ignore ISPs as if they are not present. For instance, a user who runs multiple applications (overload) with dissimilar functionalities (conflict) may become frustrated enough to skip ISPs.

Furthermore, according to Biddle (1986), role expectations are perceived based on norms, preferences, and beliefs, which can influence employee performance. Although ISPs are usually mandated in organizations, they often are perceived as extra-role activities and are not a part of their job and responsibility(Posey et al., 2014). Thus, role expectations regarding ISP demands may be given less preference to be executed when employees create their perceptions of their role expectations, including organizational tasks and security requirements. Therefore, we hypothesize that there is an inverse relationship between role stress and ISP compliance intention:

H1: Role stress decreases employee's intention to comply with ISPs.

3.2.3 Organizational commitment as a mediator between role stress and ISP compliance intention

The term commitment is defined as one's willingness to devote his/her energy and loyalty to a social system(Kanter, 1968). Organizational commitment refers to one's strong beliefs toward organizational goals/values and a desire to exert effort on behalf of the organization(Porter,

Crampon, & Smith, 1976). It also represents an employee's identification and involvement in organizations (Mowday, Porter, & Steers, 1982). Based on this perspective, organizational commitment accounts for productive security-related behaviors (Safa, Von Solms, & Furnell, 2016; Stanton, Mastrangelo, Stam, & Jolton, 2004). Employees realize that when organizations implement a set of security guidelines, it implies that ISP compliant behavior is their responsibility to ensure InfoSec in their organization. They strive to follow security rules in order to support organizational values, exhibit their loyal membership to their organizations, and do not put the organization at a security risk.

The literature on stress and employee behavior suggests that a stressful environment leads to a lack of organizational commitment (Beehr, 1998; Jena, 2015; Lambert et al., 2005). It is expected that an uncertain and unstable work environment (e.g., using uncertain and complex technologies) deviates employees from focusing on organizational objectives. For example, studies by Ragu-Nathan et al. (2008) and Low, Cravens, Grant, and Moncrief (2001) showed that employee perceived stress reduces job satisfaction, enhances burnout, and subsequently leads to low organizational commitment. Thus, we posit that organizational commitment might mediate the relationship between role stress and ISP compliance intention. That is, individuals' perception of stress resulting from role-overload, role-conflict, and role-ambiguity reduces organizational commitment. Consequently, people with low commitment are less likely to comply with ISPs and might participate in security violations. Therefore, we hypothesize that:

H2: The influence of role stress on ISP compliance intention is mediated by organizational commitment.

H2a: Role stress directly reduces organizational commitment.

H2b: Organizational commitment directly increases employee's intention to comply with ISPs.

3.2.4 Organizational support as a moderator between role stress and ISP compliance intention

In order to control the negative effects of role stress on employees' intention to ISP compliance, we explored the possibility of a factor that may mitigate stress at the workplace. Ragu-Nathan et al. (2008) assert that practical mechanisms such as organizational and technical supports are effective in the reduction of end-users' stress and anxiety at the workplace. Consistent with the literature, we propose that organizational support can be practical to mitigate adverse outcomes of role stress. Perceived organizational support refers to the extent to which employees perceive that the organization cares about them and provide required help to fulfil their needs(Eisenberger, Huntington, Hutchison, & Sowa, 1986). According to Bhattacherjee and Hikmet (2008), one aspect of organizational support is providing technical support for end-users. The availability of such organizational support can reduce employees' tension through training, providing guidance, and being accessible to resolve difficulties that employees encounter while performing role tasks(Thompson, Higgins, & Howell, 1991). It can promote affects and beliefs and serve as extrinsic motivations to desirable organizational behavior(Bhattacherjee & Hikmet, 2008).

Previous studies evidenced the positive influence of organizational supports wherein they are effective in moderating the effect of work stressors on negative psychological outcomes such as strain(Frese, 1999). Some evidence advocates organizational support reduces exhaustion and occupational stress and lowers job burnout(AbuAlRub, 2004; Jawahar, Stone, & Kisamore, 2007).

The perception of organizational support is not expected to influence employees' intention to comply with ISPs directly. Rather, it may help with the reduction of perceived stress due to the conflict and unclear duties in favor of obeying ISPs. For example, an IT assistant can provide useful instructions for a newly adopted system to reduce overload and ambiguity about its proper use. An employee with high perceptions of organizational support has more willingness to perform better

and payback the organization regardless of expending excess effort(Wang & Shu, 2008), inferring that s/he is more likely to respect organizational ISPs. Hence, we postulate that the relationship between role stress and ISP compliance intention is moderated by organizational support such that it reduces employee perceived role stress.

H3: Organizational support moderates the negative relationship between role stress on ISP compliance intention in that the negative relationship is weaker with high organizational support.

Figure 3.1 depicts our hypothesized relationships.

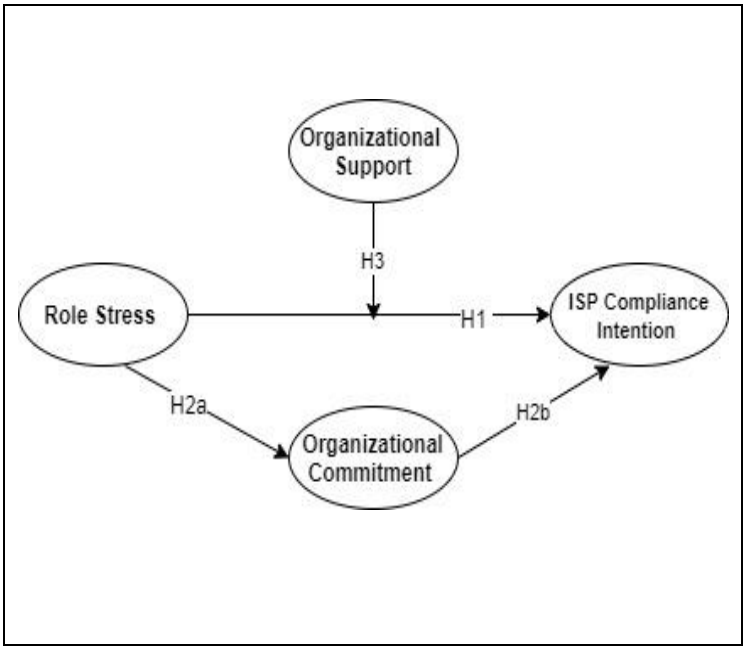

Figure 03.1 Research model

3.3 Method: measurement and sample

Measurement items were adapted from the literature. IS literature treats role stress as a second-order factor(Hwang & Cha, 2018; Tarafdar et al., 2007b) that includes role-overload, role-ambiguity, role-conflict. We adapted items for each of these factors from Tarafdar et al. (2007b)

and Ayyagari et al. (2011). Items for organizational commitment were used based on Hwang and Cha (2018). We operationalized organizational support as the availability of technical support

Table 3.1 Measurement items and item loadings

Constructs	Items	Loading
Role-ambiguity	RA1. I am unsure whether I have to deal with Tech problems or with my work activities.	0.85
	RA2. I am unsure what to prioritize: dealing with new technologies or my work activities.	0.86
	RA3. I cannot allocate time properly for my work activities because my time spent on different technologies varies.	0.78
	RA4. Time spent resolving technology related problems takes time away from fulfilling my work responsibilities.	0.59
Role-conflict	RC1. I am often asked to do things that are against my better judgment.	0.71
	RC2. I often receive an assignment without adequate resources/materials to execute them.	0.79
	RC3. I often have to bend rules or policy in order to carry out an assignment.	0.8
	RC4. I often receive incomplete requests from two or more people.	0.73
Role-overload	RO1. I often have to do more work than I can handle.	0.81
	RO2*. I am often required to do difficult tasks.	0.56
	RO3. I often work beyond actual or official working hours.	0.59
	RO4*. I often attend to many problems or assignments at the same time.	0.51
	RO5. I never seem to have enough time to do my actual work.	0.78
Organizational Support	OS1. Specialized instruction concerning the technology is available to me.	0.77
	OS2. A specific person (or group) is available for assistance with technology difficulties.	0.81
	OS3. When I need help to use technologies, guidance is available to me.	0.89
	OS4. When I need help to use technologies, specialized instruction is available to help me.	0.90
	OS5. When there is a breakdown in systems, a specialized person (group) is available immediately to fix the problem. (new developed item)	0.71
Organizational commitment	OC1. I would be happy to spend the rest of my career in this organization.	0.79
	OC2. I enjoy discussing my organization with people outside it.	0.83
	OC3. I really feel as if this organization's problems are my own.	0.80
	OC4. This organization has great deal of personal meaning for me.	0.91
Intention to ISP compliance	CI1. I intend to comply with the requirements of the ISP of my organization in the future.	0.80
	CI2. I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.	0.93
	CI3. I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	0.85

*Items removed from the analysis due to the low factor loading

within an organization and adapted items from Thompson et al. (1991). Finally, the intention to comply with ISP was measured based on Bulgurcu et al. (2010). All items used a 7-point Likert scale from Strongly disagree to Strongly agree (see Table 3.1).

Table 3.2 Descriptive statistics of survey respondents (N=350)

Factor		Frequency (%)	Factor		Frequency (%)
Gender	Male	172 (49.1)	Employment status	Full-time	290 (82.9)
	Female	178 (50.9)		Part-time	60 (17.1)
Age	< 30 years	77 (22.0)	Years of Experience	< 2 years	10 (2.9)
	31-40 years	129 (36.9)		2-5 years	45 (12.9)
	41-50	72 (20.6)		5-10 years	65 (18.6)
	>50 years	72 (20.6)		>10 years	230 (65.7)
Education	High school	85 (24.3)	Daily technology use at workplace	< 3 hours	24 (6.9)
	College	203 (58.0)		3-6 hours	133 (30.0)
	Graduate-level	62 (17.7)		>6 hours	193 (55.1)
Industry	Education	40 (11.4)			
	IT services	108 (30.9)			
	Healthcare	40 (11.4)			
	Government	22 (6.3)			
	Other	140 (40.0)			

The survey was conducted among the U.S. individuals across industries via an online research marketing company. To ensure low response bias, this platform allowed us to obtain anonymous responses from a wide range of employed professionals in different job positions. The marketing research company distributed an online survey among their panel members and requested volunteer employees to take the survey. They paid participants a small monetary reward ($0.50) for providing a complete and honest response. We used the screening technique to assure that a sample of participants represent the population of our interest, whether they possess technology-based professions. According to the company feedback, 445 people accepted the consent form to participate in the survey, which 35 respondents did not pass the screening question. Sixty responses were eliminated due to incomplete or giving incorrect answers to attention check questions. Ultimately, we used a sample of 350 responses in our analysis. Table 3.2 illustrates the demographics of our respondents.

3.4 Data analysis and results

3.4.1 Assessment of measurement validation

We used Mplus and Lavaan package of R as the primary statistical tools and conducted a covariance-based structural equation modeling (SEM) to evaluate both measurement and structural model(Kline, 2015). To assess the measurement model, we performed confirmatory factor analysis (CFA) on the entire set of items where each item was loaded on its first order construct. Then we ran a CFA for a model considering second-order role stress construct. Table 3.3 presents the results of fit indices for all models. It suggests that the data fit the models adequately since the obtained values satisfied the recommended cut-off values by Kline (2015). The close values of CFI, TLI, GFI, AGFI, and NFI to one (> 0.90) may indicate a good fit (all are sensitive to sample size, and in some software, AGFI does not perform well which is less reported in literature recently) and values between 0.05 and 0.08 for RMSEA and SRMR indicate reasonable error approximation.

While Chin (1998) recommended that majority of the items should have loadings greater than 60% (> 0.70 is ideal), the Hair, Black, Babin, and Anderson (2010) factor loading guidelines affirmed that loading of 0.35 and 0.30 are statistically significant for a sample size of 250 and 350, respectively (our sample size is 350). As Table 3.1 displays, most of items have loadings higher than 0.70 except for one item from role-ambiguity and three items from role-overload, which some are close to 0.60.

Furthermore, we examined the reliability, convergent, and discriminant validity of the constructs. A reliable measurement scale must have composite (CR) and Cronbach's alpha reliability (α) greater than 0.70 and average variance extracted (AVE) higher than 0.50 (Fornell & Larcker, 1981a). Also, discriminant validity is verified when the square root of AVE of each construct is larger than the inter-construct correlation coefficients and there is no evidence of cross loading where an item loading belonged to a latent variable does not have a higher value loaded on other latent variables (Koohang, Nord, Sandoval, & Paliszkiewicz, 2020). According to the results

Table 3.3 Goodness of fit for the measurement and structural model

Fit indices	$\chi 2$/d.f.	CFI	TLI	GFI	AGFI	NFI	RMSEA	SRMR
CFA 1	531.21/215	0.94	0.93	0.90	0.85	0.90	0.065	0.058
CFA 2	564.16/221	0.93	0.92	0.88	0.84	0.90	0.067	0.063
SEM	429.20/214	0.94	0.93	0.88	0.84	0.89	0.054	0.077

CFA 1, first order-factors; CFA 2, second-order factor; N.S., non-significant

Table 3.4 Results of construct reliability and validity

	Mean	STD	CR	α	AVE	RA	RC	RO	OS	OC	CI
RA	2.74	1.6	0.86	0.83	0.60	**0.77**					
RC	2.88	1.7	0.88	0.85	0.58	0.68	**0.76**				
RO	3.61	1.9	0.78	0.75	0.54	0.57	0.75	**0.73**			
OS	5.0	1.6	0.91	0.90	0.67	-0.29	-0.28	-0.18	**0.82**		
OC	4.4	1.7	0.90	0.90	0.70	-0.06	-0.21	-0.07	0.55	**0.83**	
CI	5.8	1.2	0.90	0.89	0.74	-0.44	-0.44	-0.25	0.31	0.22	**0.86**

CR, composite reliability; α, Cronbach's alpha reliability; AVE, average variance extracted; RA, role-ambiguity; RC, role-conflict; RO, role-overload; OS, organizational support; OC, organizational commitment; CI, compliance intention; The diagonal entries are the square root of AVE.

of Tables 3.4 and 3.5, all measures satisfy these criteria. We note that we observed accepted values of CR (0.79) and α (0.81), but a low AVE for role-overload (0.44) construct. As the inclusion of high loadings leads to high AVE(Farrell & Rudd, 2009), one reason for the obtained low AVE could be considering two items with loadings of 0.51 and 0.56 in the computation. After we removed items 2 and 4, the AVE value for role-overload increased to 0.54. Thus, these two items were removed from both measurement and structural model analyses since they improved the quality of our results. We computed AVE for the role stress by averaging the squared loadings of its three first-order factors. The obtained value was 0.71, which suggests the three first-order factors (overload, conflict, and ambiguity) explain a considerable amount of variance of role stress.

We assessed the common method bias using two approaches. First, Harmon's one-factor test(Podsakoff et al., 2003) was conducted to see whether a single factor accounts for the majority of the variance. In total, five factors emerged with the 70.5% cumulative variation with the largest of 31.4% variation which is less than a commonly accepted value of 50%.

Table 3.5 Cross loadings

	Role-ambiguity	Role-conflict	Role-overload	Compliance intention	Organizational commitment	Organizational support
RA1	0.777	0.109	-0.044	-0.05	0.02	-0.01
RA2	0.843	0.033	-0.014	-0.038	0.002	0.058
RA3	0.699	0.013	0.105	0.095	-0.039	-0.034
RA4	0.529	-0.025	0.219	-0.049	0.029	-0.089
RC1	0.164	0.709	-0.059	0.007	-0.004	0.141
RC2	0.025	0.625	0.201	-0.062	-0.061	-0.125
RC3	-0.048	0.837	0.012	0.098	0.04	0.022
RC4	0.014	0.629	0.226	-0.024	0.004	-0.092
RO1	0.072	0.389	0.438	0.005	-0.01	-0.06
RO2*	-0.078	0.045	0.743	-0.005	-0.051	0.09
RO3	0.014	0.003	0.7	-0.104	0.105	0.032
RO4*	-0.013	-0.017	0.721	0.033	0.112	-0.002
RO5	0.181	0.345	0.404	0.001	-0.035	0.029
CI1	0.012	-0.107	-0.028	0.755	-0.027	0.006
CI2	0.004	0.025	-0.009	0.948	-0.005	0.028
CI3	-0.068	-0.003	0.026	0.793	0.099	0.007
OC1	-0.005	-0.069	-0.022	0.007	0.714	0.093
OC2	-0.04	0.017	-0.042	0.039	0.772	0.082
OC3	0.035	0.058	0.007	0.01	0.841	-0.043
OC4	0.013	-0.034	0.072	-0.023	0.918	-0.011
FC1	-0.032	0.041	0.036	-0.049	0.093	0.741
FC2	0.066	-0.102	0.082	0.063	-0.031	0.788
FC3	-0.027	-0.039	0.04	0.057	-0.003	0.853
FC4	-0.067	0.117	-0.04	0.007	0.011	0.926
FC5	0.061	-0.063	-0.08	-0.016	0.061	0.676

*Items removed from the SEM analysis due to the low factor loading in CFA results

Second, according to Paul A Pavlou, Huigang Liang, and Yajiong Xue (2007) the correlation matrix (Table 3.4) does not indicate a high correlation among constructs ($r^2 > 0.90$). Therefore, the common method bias does not appear problem in our study.

3.4.2 Assessment of structural model

Next, we conducted SEM to test our hypothesized relationships. As mentioned above, we modelled the three sub-dimensions into the second-order factor, role stress, then it was related to other

constructs. As displayed in Table 3.3, fit indices verified the adequate model fit. Also, each stressor showed a significant, meaningful factor loading on role stress (see Figure 3.2). Previous research suggests individual differences could influence security-related behaviors(Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). For this purpose, we added a set of demographic factors in our model and controlled for their effects on ISP compliance intention.

The results of the standardized path coefficients, significant level, and R^2 values are presented in Figure 3.2. Role stress has a significant negative effect on ISP compliance intention (β= -0.35, $p < 0.001$) and organizational commitment (β= -0.20, $p< 0.001$). Thus, provided support for H1 and H2a. Role stress reduces employee intention to comply with ISPs and reduces organizational commitment. Also, the path from the organizational commitment to the intention of ISP compliance is statistically significant (β= 0.15, $p < 0.01$), which provided support for H2b. Organizational commitment leads to ISP compliance intention.

To ensure the presence of mediation effect in addition to verification by Baron and Kenny (1986) analysis, we performed the Sobel test for the indirect effect of role stress on ISP compliance intention through organizational commitment. We used the Preacher' online Sobel test calculator (http://quantpsy.org/sobel/sobel.htm). The Sobel test statistics was significant (Z= -2.10, $p < 0.05$). This provided support for the H2 on the mediation effect of organizational commitment and ISP compliance intention relationship. However, because the direct effect of role stress to intention is significant, based on Baron and Kenny (1986), we concluded that the path from role stress to ISP compliance intention is partially mediated by organizational commitment. We tested for the interaction effect of organizational support with role stress. The result of the analysis did not show a significant interaction effect (β= -0.08, $p >0.05$). Thus H3 was not supported. Overall, given the value of 28% for the R^2, our theoretical model demonstrated reliable explanatory power and made a meaningful interpretation.

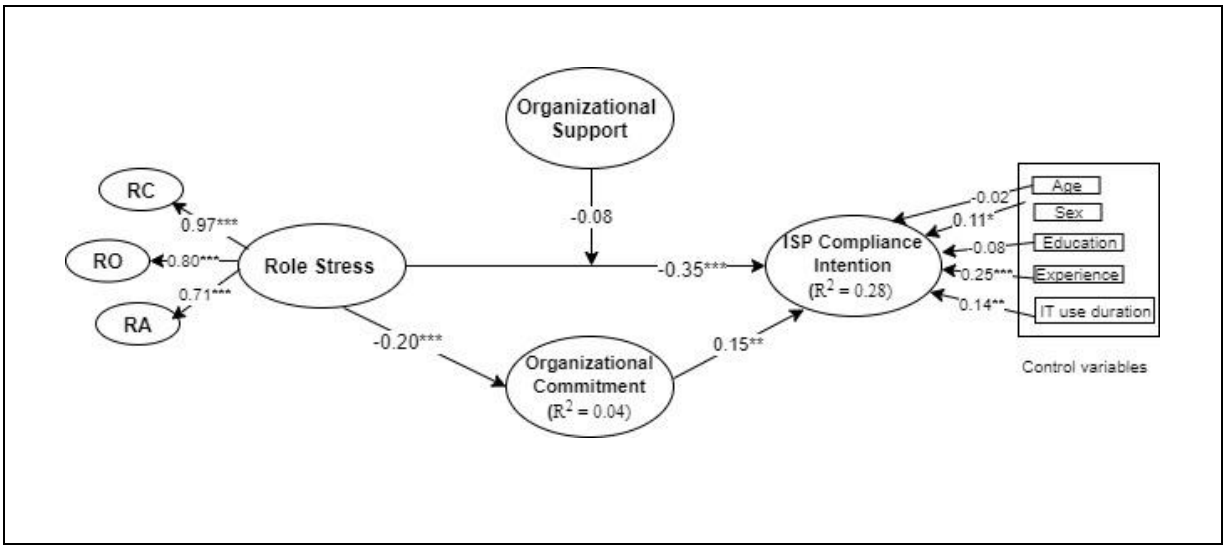

Figure 3.2 The results of the structural model testing. *p<0.05; ** p<0.01; ***p< 0.001; RA, role-ambiguity; RC, role-conflict; RO, role-overload

Furthermore, we decomposed the relationship between role stress and intention to ISP compliance into three separate relationships to provide an in-depth understanding of how each role stressor reduces ISP compliance intention. We examined a direct relationship of each stressor by regressing them on the ISP compliance intention construct independently to address the multicollinearity issue that may appear when multiple constructs are used to predict one variable(Grewal et al., 2004). All role-stressors have statistically significant negative effects on ISP compliance intention. The standardized path coefficients for each stressor and R^2 value are depicted in Figure 3.3.

3.5 Discussion, contribution, limitation

Overall, the findings of this study provided evidence on the contributed factors of employee ISP violations that the role stress arising from a combination of three stressors- *overload, ambiguity, conflict*- directly reduces individuals' intention to comply with ISPs. Furthermore, it impacts organizational commitment negatively and leads to low ISP compliance. This paper has a few *theoretical implications.*

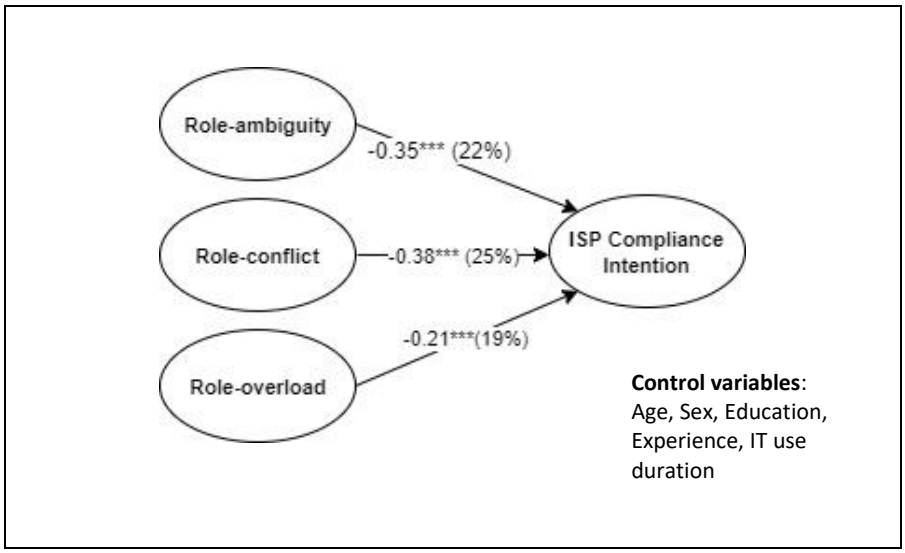

Figure 3.3 The results of the post hoc analysis, standardized path coefficients (R2); ***p< 0.001

First, it contributes to the role theory literature and the negative influence of role stress on human performance(Ayyagari et al., 2011; Guimaraes & Igbaria, 1992; Ragu-Nathan et al., 2008; Tarafdar et al., 2007b). Our results showed that the role theory, specifically organizational role theory, is a useful theoretical lens to understand security-related behaviors. Our empirical study revealed that when employees' perceived role expectations are associated with some levels of overload, ambiguity, and conflict, they could engage in non-compliant behaviors. When faced with an ISP that either levies more duties and tasks on them or is in conflict with their primary role responsibilities or is unclear or ambiguous, employees will simply choose not to comply with it. Primary roles will take precedent over extra-roles.

Second, previous research investigated the effect of security-related stress, wherein the objective of the studies is to determine how employees respond to security requirements(D'Arcy & Teh, 2019; Hwang & Cha, 2018; Teh et al., 2015). These studies applied neutralization and copying theories to explain why employees violate ISPs when they feel high complexity, uncertainty, and verload due to security requirements. Although these studies provide insightful findings, they have some limitations:

(1) The main objective of them is to address ISP compliance influenced by the stress resulting from ISP essentials, not role responsibilities. We felt it is important to extend the concept of role stress beyond the ISP requirements. Thus, in this study, we employed role theory and described how the perception of role expectations (including both intra-extra roles) could influence security-related behaviors. We postulated that it is not necessarily only ISP requirements that cause stress. Instead, role stress rooted in one's own job expectations can threaten organization security and directly influence employee security-related behaviors. Our results build on the noteworthy and commendable findings of previous researchers and depict that along with primary role stress, adding ISPs impose security-related role stress that can exacerbate the problem and worsen employees' intention to not comply.

(2) They did not evaluate and measure multiple dimensions of role stress separately. In a rare case, D'Arcy and Teh (2019) encompassed security-related stress on a 4-item scale, which has only one item to address role-conflict. In this research, we distinguished each dimension of role stress (i.e., ambiguity, overload, and conflict), conceptually defined each, explained how they might relate to ISP violations, and finally evaluated each using separate measures.

(3) They did not investigate the direct effect of role stress on ISP compliance. The study by Hwang and Cha (2018) provides an understanding of how security-related technostress leads to lower organizational commitment through security-related role stress. However, they did not look into the mediation effect of organizational commitment on the relationship of security-related role stress and compliance intention. Here, not only we examined the direct relationship between role stress (intra-extra) and ISP compliance intention, we also showed that role stress indirectly contributes to lowering compliant behaviors through organizational commitment.

Third, we decomposed the role stress construct in order to determine which dimension of role stress contributes more to ISP non-compliant behaviors. Of the three, role-conflict contributed the most

toward employee intentions of non-compliance. However, role-overload and role-ambiguity also had an effect. This is consistent with the research on intra-role and extra-role behaviors(Kim & Mauborgne, 1996; Vigoda-Gadot, 2007). As we noted earlier, primary roles will take precedent. Although some previous research reported that role-overload did not lead to stress and did not impact employee job satisfaction and organizational commitment(Coverman, 1989; Lambert et al., 2005), we found a negative direct relationship between role-overload and employee behavioral intention.

Forth, corresponding to the past research(Safa et al., 2016; Stanton et al., 2004), our results provided additional support for the impact of organizational commitment in enhancing ISP compliant behaviors. Nevertheless, we found that organizational commitment acts as a mediator between role stress and ISP compliance intention. Although high perceived organizational commitment can be considered as an affirmative factor, our study showed that role stress works as a counterproductive factor that prohibits organizational commitment to achieve its goal to enhance compliance. Finally, similar to Ragu-Nathan et al. (2008), organizational support was not found to be capable of diminishing role stress in favor of more ISP compliance. One possibility is that our subjects did not experience role stress due to technical issues as we only examined one aspect of organizational support- technical support. Also, previous findings indicated that self-report measures do not exhibit significant moderating effects on stress, and objective factors are preferred(Ragu-Nathan et al., 2008; Wall, Jackson, Mullarkey, & Parker, 1996).

For *managers and security professionals*, this study emphasized the role of occupational stress as a major contributing factor to InfoSec insider threats. Security managers might consider mitigating role-conflict through the use of technical controls rather than levy additional tasks on employees. The nurse who must respond to a code blue (intra-role) and also lock a computer down may get some relief from a technical control that would secure the device as s/he ran out of the room to provide medical assistance. Security managers might also define and describe role tasks precisely,

providing training and instructions for task requirements to avoid ambiguity, and general managers should avoid assigning more tasks than employees can handle. While that seems obvious, this research demonstrated that task overload would lead to employee non-compliance with ISPs. Managerial control for role stress not only enhances the likelihood of individuals' best security behaviors directly; it plays a role in increasing organizational commitment that results in higher secure behaviors.

We acknowledge that this study has some *limitations,* which provides avenues for *future research.* We used a subjective measure of intention to comply with ISPs. Since behavioral intentions do not entirely capture actual individual behaviors(Crossler et al., 2013), future research may consider substituting it with objective measures. In contrast with our expectations, organizational support did not act as a moderator to control role stress and promote ISP compliance. Future research should explore other stress mitigation factors. Since the perception of stress is subjective and differs by people (Penney & Spector, 2005), coping strategies such as self-efficacy (Božić, 2012) can be utilized in our proposed model to alleviate the adverse outcomes of role stress.

3.6 Conclusion

The objective of this study was to investigate one of the contributing factors of employee ISP violations. Drawing on the role theory, we examined role stress as a second-order factor of three types of stressors rooted in job role responsibilities: role-overload, role-ambiguity, and role-conflict. Our results demonstrated that role stress has a significant contribution to reducing employee intention to comply with ISPs. It also diminishes perceived organizational commitment and indirectly wards off ISP compliance. Further analysis showed that role-conflict has a stronger effect on ISP compliance intention compared to other stressors. In general, this study shed lights on the negative effect of role stress and provided fruitful insights for behavioral InfoSec scholars and professionals.

CHAPTER IV

UNDERSTANDING NON-MALICIOUS UNINTENTIONAL AND INTENTIONAL INSIDERS USING DUAL-SYSTEM THEORY: AN EMPIRICAL VALIDATION

4.1 Introduction

Information system security (ISS) is increasingly essential for organizations as security breaches are associated with monetary damage and loss of credibility (Cavusoglu et al., 2004). Despite various strategies that organizations consider to invest heavily in information security assets and infrastructure, statistical analyses show that the number of data breaches and the volume of exposed records in the US has increased in recent years (J. Clement, 2020). In agreement with Cram, D'arcy, and Proudfoot (2019), we believe that behavioral information security has taken account of many studies regarding factors that contribute to information security compliance, information security training, security awareness, and computer abuse (Bulgurcu et al., 2010; Siponen, 2000; M. T. Siponen & A. Vance, 2010; Willison & Warkentin, 2013). However, the increase in the number of security incidents rooted in human factors (Bellika et al., 2018; IBM, 2019) implies that employees continue to be responsible for the majority of breaches. Further research is required to explore and understand human behaviors.

Despite past beliefs that outsiders (e.g., hackers) are the main reason for security breaches, insiders or internal employees are the weakest link in cybersecurity as they account for more than 50% of security violations (Baker et al., 2010) and remain the top source of security incidents (Loch et al., 1992a; PWC, 2018). Except for malicious insider threats (Liang et al., 2016), where individuals

with harmful intentions deliberately attempt to hack or steal data for personal gain, insiders may violate information system security policies (ISSPs) non-maliciously in two ways: intentionally and unintentionally.

Non-malicious intentional (NMI) deviant behaviors are defined as security violations that are performed consciously against the organizational ISSPs with no malicious intent to cause destructions (Guo et al., 2011a). For example, writing down a password or sharing with a colleague, delayed backups, and installing unauthorized software are NMI. They make a conscious decision to violate ISSPs, but had no intention to cause harm. In contrast, non-malicious unintentional (NMU) violations are those end-users' behaviors that are performed unconsciously and inadvertently without harmful intentions (Ayyagari, 2012). Accidental modification of software, accidental clicks on phishing emails, and mis-delivery of sensitive data are examples of such misbehaviors. A Computer Security Institute (CSI) survey and other industry reports on information security incidents found that most of the security incidents are a result of non-malicious (intentional and unintentional) human behaviors wherein inadvertent breaches are the cause for almost 50% of the cases (Bureau, 2013; CSI, 2010; IBM, 2019; Identity Theft Resource Center, 2019) and unintentional employee threat is the most common concern reported by professionals (Posey et al., 2014).

Nonetheless, many of the ISS studies describe reasons for employees' intentional (both malicious and non-malicious) behaviors, yet there is a lack of understanding of unintentional information security misbehaviors. Although unintentional misbehaviors do not arise from malicious intentions similar to NMI misbehaviors, they are distinguishable. The former refers to misbehaviors that an insider is not aware of breaking the ISSPs since misbehaviors occur unconsciously and unwillingly through honest mistakes, but the latter refers to misbehaviors that an insider consciously chooses to perform and breaks the ISSPs on purpose. In this case, the patterns and factors that explain intentional non-malicious misbehaviors may not be appropriate or relevant to unintentional

misbehaviors. Furthermore, extant research has employed several theories to understand why employee deviate from best security practices or fail to comply with ISSPs. Such theories are the theory of planned behavior, deterrence theory, motivation-protection theory, neutralization theory, and rational choice theory (Bulgurcu et al., 2010; D'Arcy et al., 2009; Li et al., 2010; M. T. Siponen & A. Vance, 2010; Straub Jr, 1990; Warkentin et al., 2016).

The purpose of applying these theories (and others) is to identify contributing factors or determinants of employees' compliance (non-compliance) behavior with ISSPs. In other words, applied theories in ISS literature explain individuals' intentions and rational decision-making processes and may not be extendable to unintentional security misbehaviors. In the aforementioned theories, the voluntary omission of best security practices is explained by why an employee intended or decided to (not to) comply with ISSPs. Whereas conscious and rational-based theories cannot explain unintentional misbehaviors that take place when a user does not know where or when they failed to comply with ISSPs.

Our understanding of unintentional insiders is limited to definitions and a few conceptual frameworks of contributing factors (Ayyagari, 2012; Pond & Leifheit, 2003). To fill the research gap, this study proposes the dual system theory (DST) (Evans, 2003; Metcalfe & Mischel, 1999) as a theoretical framework to explain the behavioral mechanism of unintentional insiders and distinguish it from NMI. According to DST, human decisions follow two distinct cognitive systems, where individuals perform certain behaviors with either conscious (reflective) or unconscious (reflexive) mental processing. Non-malicious insiders commit ISS misbehaviors either consciously/intentionally through the reflective system or unconsciously/unintentionally through the reflexive system. To understand why insiders engage in non-malicious information security misbehaviors (NISMs) (both intentional and unintentional), we build on the prevailing DST and develop a theoretical model based on the two systems influencing employee NISMs. Given that individual risky decisions correspond to the DST(Mukherjee, 2010; Reyna & Farley, 2006), we

conceptualize the elements of DST, with a set of human factors including risk-taking behaviors, impulsivity, and curiosity. Impulsivity represents the reflexive system, and curiosity represents the reflective system, causing an outcome called conscious and unconscious risk-taking behaviors, which result in NISMs.

We assess our proposed model using an online survey from a sample of employees who had computer-based professions. Our results showed that that employees with high impulsivity (unconsciousness) and curiosity (consciousness) are more involved in conscious and unconscious risk-taking behaviors and, in turn, leading to higher NISMs. We also assert that this relationship will be moderated by perceived work-overload and information security awareness. High workload enhances the likelihood of risky decisions due to the activation of the reflexive system and results in more NISMs. High information security awareness reduces risky decisions by activating the reflective system and lead to fewer NISMs. By focusing on both intentional and unintentional NISMs, this research extends the behavioral ISS literature and introduces DST as a useful framework to explain employees' noncompliance behaviors with ISSPs.

4.2 Theoretical Background

4.2.1 Dual System Theory

Dual system theory (DST) posits that individuals' decision-making process follows two distinct systems (Evans, 2003; Lieberman, 2007; Metcalfe & Mischel, 1999; Reber, 1989; Sloman, 1996; Strack & Deutsch, 2004). In cognitive neuroscience and psychological research, these two cognitive systems are described as implicit versus explicit (Reber, 1989), conscious vs. unconscious (Sloman, 1996), automatic vs. controlled (Lieberman, 2007), and reflective vs. reflexive-impulsive (Metcalfe & Mischel, 1999; Strack & Deutsch, 2004). Drawing on these studies, we summarize the differences between two systems by referring to the terms, reflexive and reflective systems.

The reflexive system is explained as a system where processes are automatic, rapid, reflexive, and emotion-based. It involves unconscious reasoning in which a person is not aware of a mental

process. Thought processes do not engage a person's working memory, and decisions are made with very low effort. In other words, the term *automatic, unconscious mental process* refers to any process that is uncontrollable, and a person is not aware of it, and unconsciously or unintentionally will start it (Bargh, 2014). As a result, the behavior is performed automatically with no conscious attention and no deliberate control. A manifestation of the reflexive system can be represented by *impulsivity*. It refers to a personality trait that reflects a desire to act without thinking and planning for the consequences of the action (Coutlee, Politzer, Hoyle, & Huettel, 2014). A cognition process of an impulsive person is less likely to assess the situation and possible outcomes. Therefore, an impulsive person decides spontaneously through the activation of an automatic mental process (Strack & Deutsch, 2004).

Conversely, the reflective system is described as the rule-based, analytic, and the rational system in which mental processes are controllable, and a person is conscious of them. This reflective system is cognitive, emotionally neutral, and involves working memory with more slow and sequential thinking. Cognitive processes are associated with awareness and intention. Consequently, a behavioral outcome arises consciously with a high level of controls on automatic responses in the reflexive system. *Curiosity*, often understood as a positive desire or motivation associated with the recognition and self-regulation to challenge opportunities and experience novelties (Kashdan, Rose, & Fincham, 2004), represents activation of the reflective system. It is a specific form of information seeking differentiated from the fact that it is internally or externally motivated as a need for cognition (Loewenstein, 1994). Curious people seek information through conscious decision-making processes for several reasons, just as they look for food (Kidd & Hayden, 2015). Hence, a curios person decides consciously to experience and learn something by activation of the analytical system.

An interplay between the reflective and reflexive systems manifest in behavioral outcomes such as risk-taking behaviors (Trimpop, 1994). According to cognitive psychology, risk must always be

considered within a decision theory context (Kaplan & Garrick, 1981), because humans perceive risks either by the analytical system (using algorithms and formal logic) or experiential system

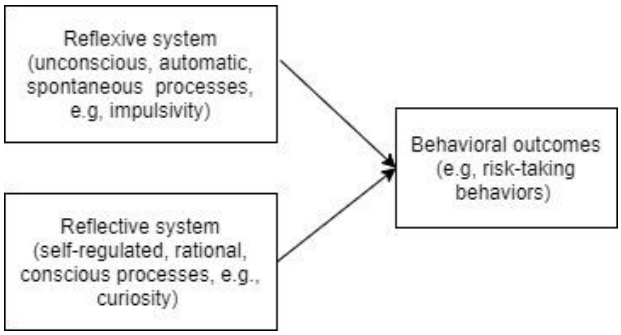

Figure 4.01. Dual System Theory

(using intuitive, quick, and automatic) mental processes (Slovic, Finucane, Peters, & MacGregor, 2004). Thus, individuals take risks based on either rational or non-deliberate/immediate decision-making processes (Reyna & Farley, 2006; Slovic et al., 2004). Figure 4.1 depicts the elements and mechanisms of the DST.

Building on DST, NISMs could be explained as an outcome of risk-taking behaviors triggered by either reflective or reflexive systems. Unintentional NISMs occur when an employee unconsciously through automatic systems, takes unconscious risks and is involved in an insecure behavior. Intentional NISMs are committed when employees decide to violate ISSPs by their own will through rational thought processes and conscious risk-taking behaviors.

4.2.2 Non-Malicious Information Security Misbehaviors (NISM)

Drawing on the behavioral ISS studies, Guo (2013) categorized security-related behaviors in terms of computer abuse (Straub Jr, 1990), security contravention (Workman & Gathegi, 2007), unethical use (Leonard & Cronan, 2001), omissive behavior (Workman, Bommer, & Straub, 2008), IS misuse (D'Arcy et al., 2009), ISSP violation (M. T. Siponen & A. Vance, 2010), and ISSP compliance (Bulgurcu et al., 2010). In a broader scope, human threats can be categorized into the internal and

external environment to the organizations, and each is divided into intentional and unintentional human actions (Loch et al., 1992a). Intentional undesirable actions within organizations are also classified based on the nature of intent: malicious vs. non-malicious. Intentional malicious behavior refers to any deliberate misuse of organizational assets by employees which puts organizations at risk of security and cause several damages like financial or reputational loss (Liang et al., 2016; Straub Jr, 1990) such as sabotage, data theft or corruption, or any cybercrime activities (Willison & Warkentin, 2013). Intentional non-malicious behavior is knowingly perpetrated by an insider who participates in unsecure volitional behaviors without malicious intent that causes damage such as password sharing and using personal devices for work purposes (Guo et al., 2011a). Unintentional ISS threats are the result of users who have authorized access to the organizational assets and unknowingly, with no malicious intent violates, the organizational ISSP (Ayyagari, 2012) such accidental clicks on phishing emails or unauthorized disclosure by inadvertent sharing of sensitive data(Khan, Kim, Mathiassen, & Moore, 2020). Since the focus of this study is to understand non-malicious unsecure behaviors, we will refer to both intentional and unintentional non-malicious behaviors and aim to distinguish them through the DST.

The similarity between these two is that both insiders are not ill-motivated and do not have harmful intentions to cause a security incident, although both increase vulnerabilities to potential threats. For example, a user may leave a PC unlocked volitionally because of the annoyance logging-in frequently (NMI). That user meant no harm but deliberately violated ISSPs. The same user may mistakenly leave a PC unlocked because of running an urgent errand (NMU). However, both misbehaviors put the organization at risk of exposure. Nevertheless, they differ to a great extent. NMI insiders break the rule (ISSPs) on purpose for their benefits such as utilitarian outcomes, normative outcomes, or saving time and effort (Guo et al., 2011a) by balancing the costs and benefits of their action through rationalization (Bulgurcu et al., 2010). In contrast, NMUs break the rules through honest mistakes without expecting any beneficial outcomes. The reasons might

be ignorance, cognitive limitations, high-risk tolerance, lack of attention knowledge, and demographic personality factors (Greitzer, Strozer, Cohen, Bergey, et al., 2014). NMUs can happen in two ways: with information security awareness and without information security awareness. On one hand, in the absence of security training and awareness, a user does not know what the expected secure behavior is. Thus, any ISSP violation can be considered as an unintentional misbehavior. For instance, if the organization does not train users that delaying software updates increases system vulnerabilities, avoiding to update is completely an unintentional and accidental error. On the other hand, when users have security awareness, they may behave fallaciously like those who are without security awareness. Some external factors can influence users' performance and put her/him in a favorable situation to unconsciously commit a violation of policy. For example, if a user is under pressure to perform multiple tasks simultaneously, s/he is more likely to click on a phishing link accidentally, without checking the sender's information.

We utilize DST to better explain the difference between these two types of non-malicious behaviors. According to DST (Evans, 2003; Lieberman, 2007), individuals' decisions to perform a particular behavior depends on the degree of awareness of a mental process and ability to control the behavior. The level of consciousness distinguishes deliberate actions from unintentional actions. Given that, non-malicious misbehaviors can be performed consciously and unconsciously. If a person unconsciously violates ISSPs, they engage in unintentional NISMs, suggesting that automatic/reflexive mental process is activated. It means that an unintentional insider is not aware of a misdeed and how and when it occurred. For example, due to a load of emails, a user may automatically click on an email, including phishing links, without thinking that it may be suspicious. On the other hand, intentional NISMs are performed by users who consciously decide to violate ISSPs. In this case, decisions follow the cognition and rational system (reflective system), which could be controlled and regulated by the users. For example, consider an employee who knows that copying organizational information to personal USB drives is against the policy.

However, s/he decides to copy information to continue the work at home in order to complete tasks faster. Therefore, employees commit NISMs through cognitive processes corresponded to DST.

4.2.3 Risk-Taking Behavior, Mechanism, and its Consequences

Risk is perceived and defined differently depending upon the objective and context of the study (Šotić, Mitrović, & Rajić, 2014) such as sociology, economic, health, management and decision making, e-commerce, information privacy, and information security (Beck, 1992; Bennett, 2010; Bodin, Gordon, & Loeb, 2008; Kim, Ferrin, & Rao, 2008; Tom, Fox, Trepel, & Poldrack, 2007; Van Schaik, Jansen, Onibokun, Camp, & Kusev, 2018). Some authors define risk as an expected loss or the tolerance of potential negative consequences to obtain higher gains (Campbell, 2005; Oppe, 1988). Some regard risk as exposure to an uncertain proposition or an inevitable behavior that changes in any environment and associated with some degree of uncertainty of the outcomes (Trimpop, 1994). It also involves future events and their consequences (Aven & Renn, 2009). For example, Kim et al. (2008) investigate the effect of perceived risk on customers' online purchasing decisions. In information security and risk management, Bodin et al. (2008) describe three facets of risk as expected loss, expected severe loss, and standard deviation of loss associated with a breach of information security. Some studies also refer to risk as users' perception of a security threat in which the magnitude of a security risk determines decisions to commit behavior (Farahmand & Spafford, 2013). Overall, the risk is defined as a degree to which an act depends on what people know about the act and is associated with uncertainty and loss or damage in some cases (Kaplan & Garrick, 1981).

Based on the definition of risk, risk-taking behavior is defined as any conscious or unconscious, controlled, or uncontrolled behavior with a perceived uncertainty about its outcome - positive or negative (Trimpop, 1994). According to the literature, risk-taking behavior appears in two ways by (1) conscious, rational decision-making processes, and cognitive assessment on risk-benefit trade-

off; and (2) non-deliberate processes with the immediate decisions (Reyna & Farley, 2006; Slovic et al., 2004; Trimpop, 1994). Stated differently, humans perceive risks either by the analytical system based on algorithms and normative rules (e.g., calculating the probability, formal logic, and risk assessment) or by the experiential system which is intuitive, quick, mostly automatic, linked by experience to emotion and affect, and not so much accessible to the conscious system (Slovic et al., 2004). For example, in the presence of danger, a person decides to (or not to) take a risk in two ways; by either fast, instinctive, and intuitive reactions or with logic, reason, and cognitive assessment toward the danger. When a person takes risk consciously, they are willing to explore and take possible challenges with no specific awareness of the outcomes. In contrast, unconscious risk-taking behavior is when the person's judgment is blurred, and for many reasons, they involve in risky behavior without fully understanding and assessing the situation. This mechanism of risk-taking behavior corresponds precisely with the description of DST, suggesting that risky decisions are processed under uncertainty by assessing outcome values through a combination of reflective and reflexive systems. (Bureau, 2013; Mukherjee, 2010; Reyna & Farley, 2006).

Risk literature denotes that risk-taking behavior cannot describe a single personality trait, and it is influenced by characteristics of the person and the situation as the result of both deliberative and affective evaluations (Figner & Weber, 2011), which suggests that risk-taking behavior may be correlated with other personality traits. People with various personality traits and individual differences engage in risky behaviors such as desirability and risk-propensity (Dewett, 2006), openness to experience and extraversion (McGhee, Ehrler, Buckhalt, & Phillips, 2012), impulsivity (Zuckerman & Kuhlman, 2000), sensation-seeking and locus of control (Bromiley & Curley, 1992), and curiosity (Kashdan, Elhai, & Breen, 2008). Among these factors, we specifically are interested in impulsivity and curiosity since both concepts have been investigated in the risk literature (Kashdan et al., 2008; Mishra & Lalumière, 2011), organizational literature (Henle, 2005; Reio Jr

& Wiswell, 2000), and ISS studies (Abraham & Chengalur-Smith, 2010; Aivazpour & Rao, 2018; Hadlington, 2017).These two factors also represent elements of the DST in this study.

Impulsivity describes a personality trait of a person who acts without thinking and planning for the consequences of the action, which often results in undesirable outcomes (Coutlee et al., 2014). Based on this definition and mechanism of risk-taking behavior, a reflective system of an impulsive person is less likely to assess the situation and possible outcomes. Therefore, an impulsive person decides automatically via activation of the reflexive system and participate in unconscious risk-taking behaviors (Mishra & Lalumière, 2011; Strack & Deutsch, 2004). Curiosity explains situations where individuals are motivated to assess existing possibilities to challenge opportunities and experience novelties (Kashdan et al., 2004). Curious people knowingly seek information and have a high willingness to take risks for the sake of exploration and experience (Zuckerman, 1979). Therefore, a curios person can be thought of as a risk-taker to experience and learn something by activation of the reflective system, regardless of the possible outcomes.

Risk-taking behaviors are associated with both negative and positive outcomes. On the one hand, risk-taking behavior in management studies demonstrates that engagement in risk results in positive outcomes, such as the circulation of financial goods (Zaloom, 2004), entrepreneurial behaviors (Barringer & Bluedorn, 1999), and productive investments (Sauner-Leroy, 2004). Moreover, employees' risk-taking behavior is correlated with high creativity (Dewett, 2007) and innovative behaviors (Yuan & Woodman, 2010). On the other hand, risk-taking behavior could be associated with adverse outcomes such as personal health loss or organizational financial loss (Yates & Stone, 1992), deviant behaviors at the workplace (O'Neill & Hastings, 2011), and organizational failure (Singh, 1986; Vaughan, 1999).

4.3 Model Development

Our proposed model presented in Figure 4.2 demonstrated that elements of the DST consisting of the reflexive system (impulsivity) and reflective system (curiosity) results in risk-taking behavior, which is a formation of the interplay between two systems. In turn, risk-taking behaviors (either conscious or unconscious) will influence NISMs. Two moderating factors of perceived work-

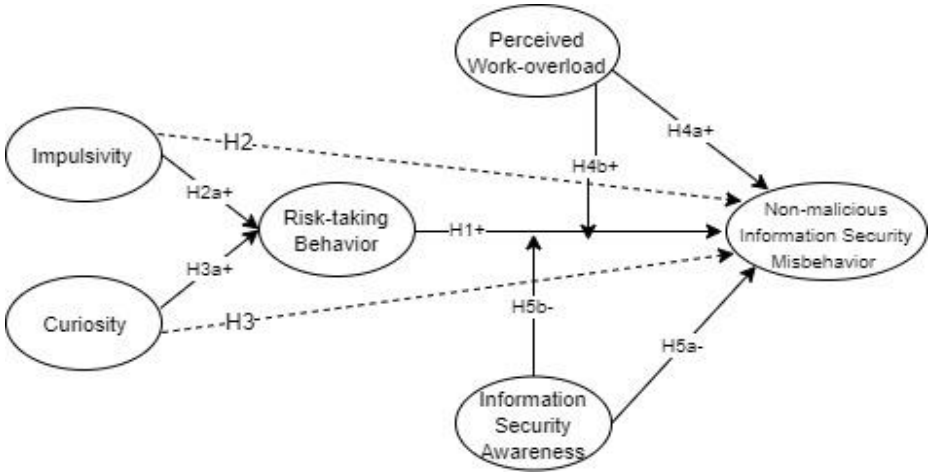

Figure 4.2 Theoretical Model (relationships with dotted lines indicate mediation effects)

overload and information security awareness will also impose negative and positive impacts on the relationship between risk-taking behavior and NISMs.

4.3.1 Risk-Taking Behavior and NISM

Risk perceptions and risky decisions are essential elements of cognitive/affective processes, which can help understand how the commitment of NISMs originates in the mind of an insider (Bureau, 2013; Greitzer, Strozer, Cohen, Bergey, et al., 2014). While using computers and networks in the workplace, employees may confront situations that make them ignore ISSPs consciously or unconsciously. Consider an employee who works on the organization's sensitive data and shares the office with his colleagues. According to the organizational ISSPs, he must lock his computer

whenever he leaves the desk. Nevertheless, because he has trust in his colleagues and finds it more convenient not to log in frequently, he consciously decides to take a risk to violate the ISSP whenever he leaves the room. Although he is aware of the potential security threats and perceives some level of a security risk (either low or high), due to the positive attitudes towards his colleagues and high willingness to make risky decisions, and in order to gain personal benefits, consciously decides to take risks and engage in intentional NISMs (reflective system). After repeating this practice for a while, this behavior becomes a habit, and ultimately, following an automatic mental system (reflexive system), he unconsciously becomes involved in risky unconscious behavior and performs unintentional NISMs. The correctness of this scenario can be confirmed relying on the studies by Colquitt, Scott, and LePine (2007) who explained people with high trust beliefs are more likely to engage in risky behaviors, and Karjalainen, Sarker, and Siponen (2019) who explain the nature of employees' decisions to perform ISS behavior is dynamic and changes over time.

In another circumstance, employees take risks when using employer-issued devices at home for personal activities (e.g., online shopping) or use unsecured Wi-Fi to be available when they work remotely. It is also probable that an employee due to the negligence without consciously verifying the information of senders takes a risk and accidentally infects a system by mistakenly clicking in a phishing scam (D. P. Biros, M. Daly, & Gunsch, 2004). Usually, hypersensitive employees who have a fear of being criticized have a low-risk propensity and double-check anything they do in order to reduce their risky behaviors (Lukacs, Negoescu, & David, 2009). In contrast, people with high-risk propensity do not assess outcomes of their actions, and regardless of what the consequences are, immediately take action. One employee may consciously take a risk and through rationalization (Bulgurcu et al., 2010; Li et al., 2010) and neutralization (M. T. Siponen & A. Vance, 2010) of his/her behavior participates in intentional NISMs. Alternatively, in particular situations (e.g., finishing a task immediately), they may engage in unintentional NISMs where his decisions are made automatically with no awareness of possible consequences of the behavior. We

acknowledge that risk-taking behaviors can relate to unintentional NISM only when users, to some extent, have security awareness. If a user was never taught security violations, risk-taking behaviors would not be reasonable because all NISMs are unintentional, practically related to unconscious risks. Here, we assert that a well-informed user may contribute to unintentional NISMs due to the high willingness to take risks by the unconscious decision making process.

Overall, past research indicated that employees who typically are risk-takers they are more likely to contribute in adverse organizational outcomes (O'Neill & Hastings, 2011; Singh, 1986; Vaughan, 1999) as well as falling to phishing (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). Also, people who are lesser risk-takers in their personal life regarding health and safety, pay more attention to update security patches and to secure their devices (Gratian et al., 2018). Hence, we hypothesize that employees with high risk-taking behaviors at the workplace are more likely to perform intentional and unintentional NISMs through the conscious and unconscious decision-making process.

Hypothesis 1: Risk-taking behaviors are positively related to NISMs.

4.3.2 Impulsivity, Curiosity, and NISM

Impulsive behaviors give rise to adverse outcomes at the workplace, such as employees' deviant behaviors, lack of self-discipline, workplace violence, and employment instability (Henle, 2005). In ISS literature, Hadlington (2017) and Egelman and Peer (2015) found a negative relationship between impulsivity and security behaviors, and in particular cases, it relates to phishing susceptibility (Welk et al., 2015). Although these studies examined the direct relationship between impulsivity and nonsecure behaviors, some research showing individuals with high levels of impulsivity are more likely to take a risk with a low perception of hazards (Coutlee et al., 2014; Zuckerman & Kuhlman, 2000). This suggests that impulsive people underestimate the potential security risks associated with misbehaviors. An impulsive insider without forethought may take

risks and engage in NISMs through activation of the reflexive system, considering that the probability of a security threat is low and no potential harm will be arisen from deviation of ISSPs. Given that impulsive people are more risk-takers (discussed in section 2.3) and risk-taking behaviors leads to NISMs (H1), we expect that the impact of impulsivity on NISMs will be mediated through risk-taking behaviors. In fact, impulsivity may not be a predictor of NISMs by itself, but can result in NISMs by triggering unconscious risk-taking behaviors (full mediation effect).

Hypothesis 2: The effect of impulsivity on NISMs will be fully mediated through risk-taking behaviors in such impulsivity positively relates to risk-taking behaviors (H2a), and risk-taking behaviors positively relate to NISM (H1).

Curiosity is considered a valuable workplace personality trait since it enhances employees' job performance through motivations towards exploration and learning (Reio Jr & Wiswell, 2000). Contrarily, it may become a potential security threat and lead to security incidents. End users who like to explore networks, browse websites, or install advanced software or programs (especially for personal activities with work devices) knowingly seek to gain knowledge and contribute to conscious risky behaviors. Ultimately, they may non-maliciously contribute to ISSP violations and accidentally corrupt systems and increase the vulnerabilities of ISS incidents. Sometimes, curiosity can be sufficient by itself to motivate an employee (via activation of the reflective system) to take advantage of his capabilities to violate ISSPs just for gaining knowledge and, as a matter of eagerness, takes a known risk to see what really can happen (Sarkar, 2010). Moreover, curious insiders are the main target of malicious insiders to lure and attract them by using curiosity-exploiting subject lines to open malicious e-mail attachments or phishing links (Abraham & Chengalur-Smith, 2010; Moody, Galletta, & Dunn, 2017). From the prior discussions, we expect that curiosity will prompt individuals to make risky decisions, and in turn, risky decisions induce employees to engage in NISMs. Therefore, we hypothesize that:

Hypothesis 3: The effect of curiosity on NISMs will be fully mediated through risk-taking behaviors in such curiosity positively relates to risk-taking behaviors (H3a), and risk-taking behaviors positively relate to NISM (H1).

4.3.3 Perceived Work-overload and NISM

Perceived work overload is the perception that a person has too much to do, and available resources are not sufficient to accomplish tasks (Leiter & Schaufeli, 1996). It happens when a person perceives that the assigned work is more than his capability or skill level (Moore, 2000). In this case, he needs to accomplish tasks under time pressure to meet deadlines, which makes him feel overloaded. As a result, due to the limited capacity of cognitive system (working memory) to process information, perceived work-overload will lead to low-quality employee performance in terms of decisions and reasoning (Eppler & Mengis, 2004), feeling stressed (Ayyagari et al., 2011), engagement (Okolo, 2018), job turn over (Moore, 2000), organizational commitment (Ahuja, Chudoba, Kacmar, McKnight, & George, 2007), and IT adoption and innovativeness with IT (Pennington, Kelton, & DeVries, 2006). Regarding information security, scholars found that ISS requirements increase workload with adding additional tasks (e.g., updating patches) and make employees feel stressed and be interrupted to perform their primary job tasks and as a result, intention to violate ISSPs increases (Albrechtsen, 2007; D'Arcy et al., 2014).

According to the mechanism of decision making through the DST (Evans, 2003), employees are inclined to follow the reflexive system under perceived work-overload. Due to the feeling stressed and time pressure to accomplish tasks, employees are less likely to decide through high-quality reasoning, deeper cognitive processing, and rationalization (Eppler & Mengis, 2004; Turel & Qahri-Saremi, 2016). Stressful situations resulting from high workloads disrupt rational and deliberative mental processes, and decisions are more intuitive and automatic (Porcelli & Delgado, 2009). For example, consider a person who receives too many emails in a day for communicating

and integrating multiple tasks. It is highly probable that due to a large number of received emails, individuals' recognition of detecting phishing emails be reduced, and accidental clicks on phishing links give rise to unintentional NISMs. In another case, an employee may intentionally ignore ISSPs (NMI) because their priority is to accomplish job tasks instead of performing ISS requirements. A non-risk-taker in a typical workday who attempts to comply with ISSPs, when in conditions of work overload, may have to take risks and non-maliciously violate security regulations. Therefore, we expect that perceived work-overload increases the likelihood of NISMs by itself and also increases the propensity of employees to make risky decisions and consequently involve in NISMS.

Hypothesis 4a: Perceived work-overload is positively related to NISMs.

Hypothesis 4b: Perceived work-overload will positively moderate the relationship between risk-taking behaviors and NISMs.

4.3.4 Information Security Awareness and NISM

Many security errors occur with a low-level understanding of the right action. While ISS scholars emphasize the role of information security awareness on the enhancement of compliance with ISSPs and effective security management program (Bulgurcu et al., 2010; Siponen, 2000), IDG Research services reported that the majority of organizations in the U.S. provide security awareness training to their employees, but 29% of organizations train only once a year (IDG Research, 2018). Information security awareness is defined as an employee's general knowledge about information security and the organization's security objectives (ISSPs) (Bulgurcu et al., 2010; Siponen, 2000). The goal of awareness is to reduce the number of security errors in terms of protection, integrity, and information confidentiality. A wide range of ISS studies have shown that information security awareness changes employee's information security behaviors. Recently, Cram et al. (2019) conducted a meta-analysis to identify antecedents to ISSP compliance. In 27 studies (out of 95

papers included in the meta-analysis), security training and awareness (SETA programs) is one of the identified categories with a medium/large effect size. We explored each of these empirical studies to look at the role of security awareness in security-related behaviors. Except for three studies by Abed, Dhillon, and Ozkan (2016), Brady (2010), and Donalds (2015) which examined the effect of security awareness on the intention to general ISSP compliance, in all studies, the information security awareness construct has an indirect effect on security behaviors as a predictor of attitudes, beliefs, perceived sanctions, rewards, and other outcomes (D'Arcy, 2005). Considering the findings of Cram et al, (2019), the direct effect of information security awareness on NISMs is less known.

Despite prior studies which described that security awareness develops attitudes toward intention to compliance over time (Bulgurcu et al., 2010), we argue that a user with a higher level of security awareness is less likely to contribute in NISM because they are well-informed about potential threats that arise from insecure behaviors and are educated not to commit in ISSP violations or insecure decisions. A user may not be aware of the risk of public Wi-Fi or opening unreliable links and attachments, and due to unconsciousness, may become involved in unintentional NISMs. Security training, like anti-phishing training programs, can be useful in identifying fraudulent websites (Sheng et al., 2007). Moreover, an insider who is used to ignoring secure behaviors and violates ISSPs non-maliciously for his benefits (e.g., to save time and accomplish tasks faster) with a high-security awareness will be able to regulate his personal preferences through rationalization. The analysis of perceived benefits compared to perceived costs associated with either ignorance or compliance can result in less insecure decisions and behaviors (Li et al., 2010). Therefore, we argue that a user with a high level of security awareness is better able to utilize cognitive mental processing to better avoid NISMs.

Furthermore, information security awareness can alleviate risk-taking behaviors. Risky beliefs and risky behaviors are consequences of a users' lack of security awareness (Badie & Lashkari, 2012).

Given the DST, a knowledgeable risk-taker user is better able to assess uncertain outcomes associated with his insecure behaviors (using the reflective system) and is capable of controlling his willingness to take a risk whenever he aims to perform NISMs. Recently, McCormac et al. (2017) found that there is a negative correlation between risk-taking behavior and information security awareness wherein individuals with high information security awareness take fewer risks. SETA programs can be successful at enhancing employees' recognition of security threats and cognitive biases that affect risky decision making (Bureau, 2013). In sum, we hypothesize that:

Hypothesis 5a: Information security awareness is negatively related to NISMs.

Hypothesis 5b: Information security awareness will negatively moderate the relationship between risk-taking behaviors and NISMs.

4.4 Methodology

4.4.1 Measurement

We utilized an online survey instrument to collect data. Respondents received a set of questions designed to measure the proposed model constructs. Drawing on the literature, we selected an initial set of items and then modified some (as needed) in order to reflect our proposed model. Curiosity was measured with ten items adapted from Mussel, Spengler, Litman, and Schuler (2011). We deliberately choose this scale as it measures employees' work-related curiosity since we are interested in human behavior at the workplace. Similarly, we measured individuals' work-related risk-taking behaviors using eight items adapted from Dewett (2006). Impulsivity was measured using 13 items from Coutlee et al. (2014) that tapped into attention, motor, and non-planning dimensions of impulsivity. To measure NISMs, we used a scale developed by Hadlington (2017). This scale addresses the main and common ISS violations based on ISS literature (D'Arcy et al., 2014; Egelman & Peer, 2015) such as password sharing and choosing, using insecure USB devices or online storage systems, failing to update software, using unsecured wireless networks, and

clicking links without verifying the source. This scale consists of 20 items, although we only used 14 of them and removed the other six for some reasons: First, keeping a scale short is effective to reduce response bias (Hinkin, Tracey, & Enz, 1997). Second, some questions concern individuals' personal life, and we are interested in behaviors in a professional setting. Finally, we limited questions to employees' online behaviors at the work-place since digitization has changed the nature of work (Forman et al., 2014), and most of the job-tasks are performed through online platforms (Gloster, 2018). We believe many of NISMs include unsafe online behaviors. We measured perceived work-overload using four items applied in the Moore (2000) study. Items for information security awareness were taken from Bulgurcu et al. (2010). The items and scales used in this study are presented in Appendix 4. A.

4.4.2 Sample

To collect data, we used a crowdsourcing market research company located in the United States to distribute the survey among participants. This platform allows us to collect anonymous responses that are preferred to provide honest and desirable responses. The respondents were selected from a wide range of industries and job positions to provide a heterogeneous sample to address organizational or cultural differences (Bulgurcu et al., 2010). After completing the consent form, respondents were asked to pass a screening question to ensure they have computer-using professions and then were allowed to continue to answer survey questions. Upon completion of the survey, they received a small monetary reward. We eliminated 44 responses due to incomplete responses (i.e., fail to answer attention check questions or unreasonable survey completion time). In the end, we included 301 usable responses in our data analysis. Of the sample of 301 respondents, 59 percent were male, 39 percent were between 31-40 years old, and around 43 percent had the daily internet usage of more than six hours at the workplace. Also, 93 percent of respondents had high information security knowledge which provided the valid sample to assess our proposed model (i.e., in case of committing unintentional NISMs, the reason is not because of the lack of awareness,

instead other predictors detect the level of contribution to unintentional NISMs). The mean value for each items of the information security awareness scale was also calculated (See Appendix 4.A). All values were above 4.1 (out of 5) which implied that most of the respondents reported that for each individual item they had high levels of awareness. Table 4.1 reports sample demographics.

Table 4.1. Descriptive Statistics of Survey Respondents (N=301)

		Frequency	**Percentage**
Gender	Male	178	59
	Female	123	41
Age	18-30 years	83	28
	31-40 years	119	39
	41-50 years	50	28
	51-60 years	36	17
	Above 60 years	13	12
Education	High School or equivalent	75	25
	College graduate	167	55.4
	Higher-Education	49	14.5
	Other	10	3.3
Employment status	Full-time	271	90
	Part-time	27	9
	Unemployed	3	1
Years of experience	Less than 2 year	3	1
	2-5 years	38	13
	5-10 years	64	21
	Above 10 years	196	65
Industry	Education	34	11.2
	IT Services	73	24.3
	Healthcare	30	10
	Government & Non-Profit	34	11.3
	Other	130	43.2
Daily Internet usage at the workplace	Less than 3 hours	47	15.6
	3-6 hours	125	41.5
	More than 6 hours	129	42.9
Level of overall awareness of organizational information security (scale of 1-5)	Low (<=2)	13	4.3
	Medium (=3)	8	2.7
	High (>=4)	280	93

4.5 Data Analysis and Results

We used Mplus as the primary statistical tool to analyze the measurement and structural models. Since the nature of our study is theory testing in the context of predictive modeling, a covariance-based technique- structural equation modeling (Ullman & Bentler, 2003) is well suited for our research to analyze latent variables and their relationships.

4.5.1 Measurement Model

To evaluate psychometric properties and quality of measurement scales, we examined model fit, individual item reliability, convergent validity, composite reliability, and discriminant validity of the measurement model (Donald Barclay, Christopher Higgins, & Ronald Thompson, 1995) before testing the structural model as recommended by Anderson and Gerbing (1988).

First, to test whether the data fit the measurement model, we performed a confirmatory factor analysis on each construct separately and then on the entire set of items (Brown, 2015). One dimension of the impulsivity construct (motor) did not show a good fit. All items in the first-order motor construct had deficient loading factors (less than 0.5) and weak fit indices (Chin, 1998). In order to obtain a good fit, we removed those four items as well as one from perceived work-overload and one from the NISM construct. As a result, the finalized measurement model satisfied the threshold of good model fit corresponded to Ayyagari et al. (2011), suggesting that the data fit the model well. Results of CFA- fit indices (CFI, RMSEA, SRMR) are reported in Table 4. 2. All values are above/below the cutoffs of 0.90 for CFI, 0.10 for SRMR, and 0.10 for RMSEA (Kline, 2015).

Table 4.2 Goodness of Fit Assessment for the Measurement and Structural Models

Goodness of fit measures	χ^2 (d.f.)	χ^2 /d.f	CFI	RMSEA	SRMR
Good model fit ranges	Non-sign.	< 2.00	> 0.90	< 0.1	< 0.1
CFA Model	1873 (1014)	1.84	0.91	0.053	0.063
SEM Model	1875(1016)	1.84	0.91	0.053	0.064

Second, we examined factor loadings of items belonging to each construct and the average variance extracted (AVE) to test item reliability and convergent validity of constructs. As reported in Table 4.3, all of the measurement item loadings are above the recommended value of a minimum of at least 0.50 (good) and 0.60 (very good), indicating 50% or more of the shared variance with the construct (Chin, 1998). Except for NISMs with AVE of 0.48, the obtained AVE values for all reflective constructs support convergent validity by exceeding the minimum required value of 0.50 (Chin, 1998). The low AVE could be a result of consideration of two factors in its computation: low factor loadings less than 0.60) and a large total number of items in the construct (Farrell & Rudd, 2009).

Third, to ensure the scale reliability, we assessed Cronbach's alpha reliability and composite reliability. From Table 4.3, the scores for Cronbach's alpha ranged from 0.76 to 0.93 and for composite reliability ranged from 0.79 to 0.94, which all are higher than the acceptable value of 0.70 (Gefen et al., 2000). Finally, to confirm the discriminant validity of constructs in our model, the square root of the AVE for each construct was calculated. It is recommended that AVE value to be higher than the inter-construct correlation scores in order to show that constructs are loaded on their focal constructs and less on others (Fornell & Larcker, 1981b). As presented in Table 4.4, the diagonal values (square root of AVE) in the constructs' correlation matrix all are larger than off-diagonal correlations. Consequently, the results of Tables 4.2, 4.3, and 4.4 demonstrate supportive evidence for the validity and reliability of our measurement model.

It is recommended to evaluate common method bias when the independent and dependent variables in a study are measured using the same instrument (Podsakoff et al., 2003). To assess the potential common method bias in our model, we performed Harman's one-factor test (Podsakoff et al., 2003) and a test by Paul A Pavlou et al. (2007) to examine the correlations between constructs. In Harman's one-factor analysis, the goal is to observe whether a single factor emerges or one single factor explains a large amount of the variance. After conducting the test, eight factors emerged with

Table 4.3 Confirmatory Factor Analysis and Statistics

Standardized latent constructs loadings										
Latent variable	Item	CUR α= 0.92	IMP α= 0.88	RTB α= 0.93	NISM α= 0.92	PWO α= 0.76	ISA α= 0.91	R^2	CR	AVE
Curiosity (CUR)	Cur1	0.55						0.31	0.92	0.55
	Cur2	0.74						0.54		
	Cur3	0.73						0.53		
	Cur4	0.81						0.65		
	Cur5	0.79						0.62		
	Cur6	0.73						0.53		
	Cur7	0.75						0.56		
	Cur8	0.70						0.49		
	Cur9	0.81						0.65		
	Cur10	0.79						0.62		
Impulsivity (IMP)	Imp1		0.86					0.75	0.92	0.59
	Imp2		0.68					0.46		
	Imp3		0.65					0.42		
	Imp4		0.69					048		
	Imp5		0.77					0.60		
	Imp6		0.69					0.47		
	Imp7		0.87					0.76		
	Imp8		0.87					0.76		
Risk-taking Behavior (RTB)	Rtb1			0.76				0.57	0.94	0.66
	Rtb2			0.77				0.59		
	Rtb3			0.82				0.67		
	Rtb4			0.85				0.72		
	Rtb5			0.70				0.48		
	Rtb6			0.85				0.72		
	Rtb7			0.86				0.75		
	Rtb8			0.89				0.79		
Non-malicious Information Security Misbehavior (NISM)	Nism1				0.73			0.53	0.92	0.48
	Nism2				0.72			0.52		
	Nism3				0.54			0.30		
	Nism4				0.54			0.29		
	Nism5				0.73			0.54		
	Nism6				0.57			0.32		
	Nism8				0.79			0.62		
	Nism9				0.66			0.43		
	Nism10				0.73			0.53		
	Nism11				0.84			0.71		
	Nism12				0.69			0.48		
	Nism13				0.67			0.45		
	Nism14				0.72			0.51		
Perceived Work-overload (PWO)	Pwo1					0.80		0.65	0.79	0.56
	Pwo2					0.79		0.63		
	Pwo4					0.63		0.40		
Information Security Awareness (ISA)	Isa1						0.80	0.64	0.91	0.67
	Isa2						0.81	0.65		
	Isa3						0.84	0.70		
	Isa4						0.83	0.70		
	Isa5						0.81	0.65		

Table 4.4 Latent variable Statistics

	Mean	Std. Dev.	CUR	IMP	RTB	ISA	PWO	NISM
CUR	4.01	0.94	**0.74**					
IMP	2.1	0.97	-0.73	**0.77**				
RTB	3.1	1.8	0.34	-0.10^{+}	**0.81**			
ISA	4.2	0.85	0.63	-0.52	0.21	**0.82**		
PWO	2.86	1.88	-0.11^{+}	0.22	0.1^{+}	-0.12	**0.74**	
NISM	1.7	1.1	-0.23	0.18	0.11	-0.34	0.33	**0.69**

the 60% of cumulative variation with the largest of 24% variation for a single factor, which is less than the commonly accepted threshold of 50%. These results confirm that common method bias is not a serious issue in this study. Following Paul A Pavlou et al. (2007), we performed a test to calculate correlations between constructs of our model to see if there is a high correlation among constructs ($r^2 > 0.90$). According to the results of Table 4.4, none of the constructs are extremely correlated to each other. This provides additional support that common method bias does not pose a threat to our analysis.

4.5.2 Structural Model

Since we were ensured of the adequate reliability and validity of our constructs, we tested the hypotheses by performing path analysis through structural equation modeling (Byrne, 2013). The results of the structural model, including standardized path coefficients, the significance of the path coefficients, and the amount of explained variances (R^2) are shown in Figure 4.3. Based on the significance of path coefficients and corresponding effect sizes, all hypotheses were supported and exhibited meaningful path coefficients (Chin, 1998). The structural model explained 39% of the variance related to non-malicious information security misbehaviors and 17% related to risk-taking behaviors. The significant positive effect of risk-taking behaviors on NISMs ($\beta = 0.21$, $p<0.001$) provides support for H1. Risk-taking behavior is positively related to NISMs. The significant positive effects of impulsivity ($\beta = 0.35$, $p<0.001$) and curiosity ($\beta = 0.60$, $p<0.001$) on risk-taking

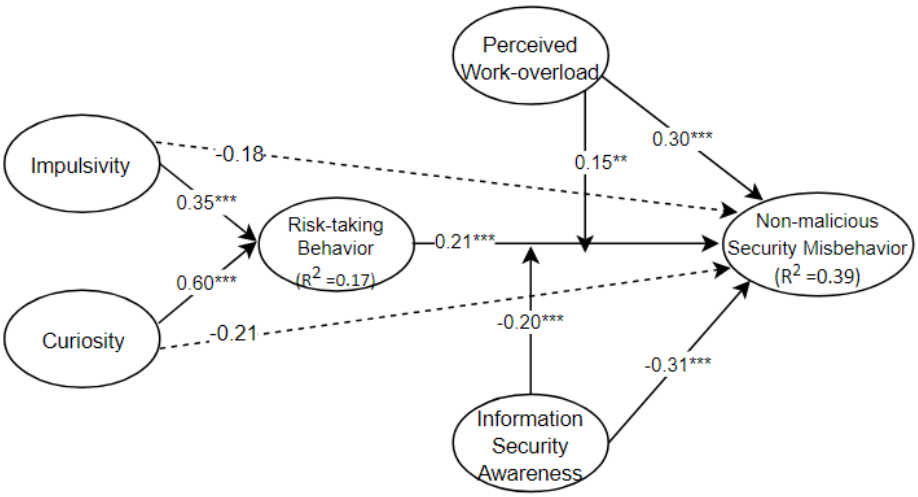

Figure 04.3 The Results of the Structural Model Testing

behavior provide support for H2a and H3a. Curiosity and impulsivity are positively related to risk-taking behaviors. Additionally, the direct path from both impulsivity and curiosity to NISMs was not significant, suggesting complete mediation, according to Baron and Kenny (1986). Furthermore, we performed the Sobel test using Preacher's online calculator (http://quantpsy.org/sobel/sobel.htm). The Sobel test statistics for the relationship involving curiosity (Z= 3.31, $p < 0.001$) and impulsivity (Z= 2.57, $p < 0.01$) were both significant. Therefore, H2 and H3 were supported. The effect of impulsivity and curiosity on NISMs is fully mediated by risk-taking behaviors.

The significant positive effect of perceived work-overload on NISMs supports H4a (β= 0.30, $p<0.001$). Perceived work-overload is positively related to NISMs. Also, the positive significant moderation path (β= 0.15, $p <0.01$) of perceived work-overload on the relationship between risk-taking behavior and NISM provides support for H4b. Furthermore, the significant negative effect of information security awareness on NISMs supports H5a (β= -0.31, $p<0.001$). Information security awareness is negatively related to NISMs. Finally, results showed that information security

awareness had significant interaction with risk-taking behavior (β=- 0.20, p<0.001) to influence NISMs, which provides support for H5b.

In order to realize the interaction effects, we plotted the significant interactions following Aiken, West, and Reno (1991). Figure 4.4(a) and 4.4(b) show how perceived work-overload and information security awareness interact with risk-taking behaviors. Figure 4.4(a) illustrates the simple slopes of NISMs on Risk-taking behaviors at high and low values of information security awareness. The results of the slope test show that when security awareness was low, risk-taking behavior had a positive effect on NISMs. When security awareness was high, the relationship between NISMs and risk-taking behaviors became less strong and almost flat, meaning that higher levels of information security awareness tend to mitigate the influence of risk-taking behavior on NISMs. The results indicate that risk-taking behavior was effective in increasing NISMs when the level of individuals' security awareness was low.

Additionally, Figure 4.4(b) illustrates the simple slopes of NISMs on risk-taking behaviors at high and low levels of perceived work-overload. These results indicate that the relationship between NISMs and risk-taking behavior became stronger and positive under the condition of a higher level of perceived work-overload.

4.6. Discussion, Implications, and Future Research

4.6.1 Discussions of the Findings

We examined the antecedents of one crucial aspect of behavioral information system security (ISS), namely non-malicious information security misbehaviors (NISMs). We drew on dual systems theory (DST) to distinguish intentional and unintentional NISMs. We posited that impulsivity and curiosity could be representatives of the reflexive and reflective systems of the DST, which lead to risk-taking behaviors (i.e., an outcome of the interplay between two systems). Then we developed

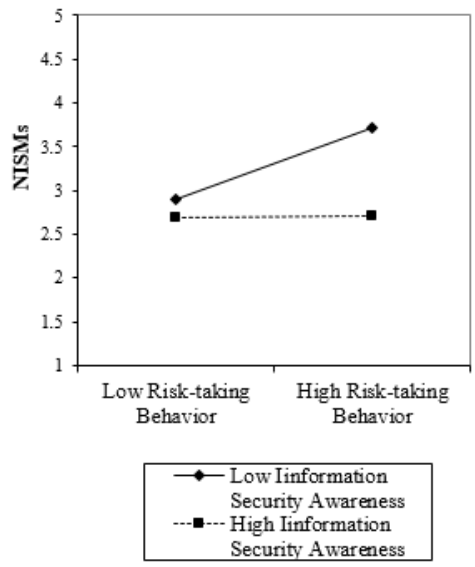

Figure 4.4(a). Riks-taking behavior × Information Security Awareness

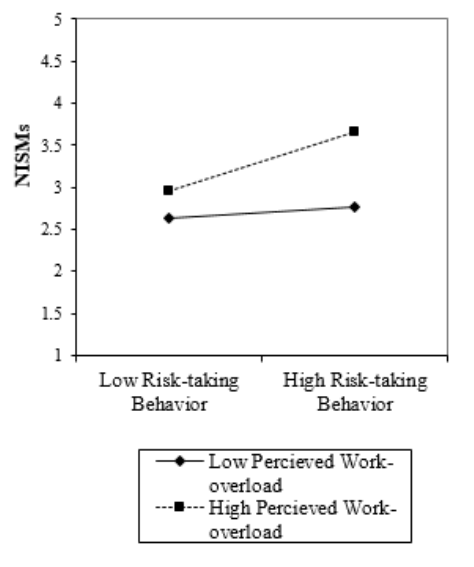

Figure 4.4(b). Riks-taking behavior × Perceived Work-Overload

Figure 4.4 Interactions of Perceived Work-overload and Information Security Awareness with Risk-Taking Behaviors

the logic for why risk-taking behaviors would impact employees' NISMs. We endeavored to understand the role of employees' risk-taking behaviors (conscious and unconscious) in influencing intentional and unintentional NISMs originated by the activation of either reflexive or reflective systems. Furthermore, we showed that individuals' perceived work overload and information security awareness interacted with risk-taking behaviors in affecting NISMs. Based on the data collected from 301 employees, all the hypotheses were supported.

Consistent with the proposed research model, we found that employees who have a high willingness to take risks in the workplace are more likely to violate ISSPs either intentionally or unintentionally through the utilization of cognitive and automatic mental processes. Previously, Moody et al. (2017) had found that individuals with high-risk propensity and curiosity are more likely to click on phishing emails. Our results generalized this finding to a set of NISMs and indicated that risk-taking behaviors mediate the relationship between NISMs and both impulsivity and curiosity. This

suggests that impulsive and curious employees are likely to engaged in risky behaviors and ultimately lead to non-malicious information security violations. Previously, scholars found that impulsivity has a direct effect on risky cybersecurity behaviors (Aivazpour & Rao, 2018; Hadlington, 2017). However, our results from mediation analysis showed that impulsivity does not influence NISMs per se; instead, it triggers risk-taking behaviors and ultimately leads to NISMs.

We found that employees' perception of high work-overload leads to more NISMs. Also, perceived work-overload positively interacts with risk-taking behaviors and enhances employees' willingness to become involved in NISMs. Moreover, as we hypothesized, information security awareness has a negative influence on NISMs and plays an essential role in reducing NISMs due to the negative interaction with risk-taking behaviors. Interestingly, our statistical findings report that the positive impact of information security awareness in NISM reduction is negated by perceived work-overload, suggesting that organizational effort in enhancing employee information security awareness can be simply offset by high levels of workload.

4.6.2 Theoretical Contributions

Our work makes several contributions to the field of ISS research. First, the majority of behavioral ISS literature has investigated the theory of planned behavior, deterrence theory, motivation-protection theory, and neutralization theory to identify root causes of intention to non-malicious information security violations. To the best of our knowledge, this is the first study that utilizes DST in order to provide a theoretical explanation and empirical support for the impact of some individual factors on NISMs. We demonstrated that DST is appropriate in the NISM context to understand how employees decide to (not to) commit misbehavior intentionally and unintentionally through the employment of reflective or reflexive mental processes. An alternative theory to DST that has been applied in ISS studies could be a rational choice theory (Bulgurcu et al., 2010). However, rational choice theory only focuses on rationally decision-making processes through cost-benefit analysis to explain intentional NISMs and cannot address unintentional or unconscious

NISMs. Therefore, DST can fill this gap. Scholars previously have adopted DST as a theoretical basis in IS research, such as social networking sites and technology use (Liu, Wang, Min, & Li, 2019; Turel & Qahri-Saremi, 2016). This study revealed that the DST is appropriate to be employed in ISS context too.

Second, most behavioral ISS studies have attempted to explain intentional ISSP compliance or non-compliance behaviors, either malicious or non-malicious. Given that the majority of security breaches are unintentional (IBM, 2019), our knowledge of unintentional misbehaviors is limited. There are a few non-empirical studies regards to unintentional violations that have provided only definitions, examples, and possible contributed factors of unintentional ISS misbehaviors (Greitzer, Strozer, Cohen, Bergey, et al., 2014; Loch et al., 1992a). Drawing on DST, we distinguished between intentional and unintentional non-malicious information security misbehaviors and offered a theory-based description of unintentional NISMs. Furthermore, despite many behavioral studies which use user intentions to measure the dependent variable, we measured self-assessed employees' actual act of NISMs.

Third, this study extends prior research on understanding human factors contributed to employees' security-related behaviors. Prior research has primarily focused on individual differences in terms of beliefs, attitudes, some personality traits (e.g., big five model), and demographic factors (Anwar et al., 2017; Hadlington, 2017; McCormac et al., 2017). We extend this work by leveraging some personality traits such as risk-taking behaviors, impulsivity, and curiosity to study their potential consequences in the context of NISMs. Moreover, there have been recent calls in the IS field for studies focusing on the psychology of insiders and the role of human factors, especially risk-taking behaviors (Bureau, 2013; Greitzer, Strozer, Cohen, Bergey, et al., 2014; Li et al., 2019; Sarkar, 2010). In this study, we added to prior research and addressed recent calls. We empirically showed the problematic aspect of employees' risk-taking behavior as a threat to information security. Furthermore, we found that impulsivity and curiosity have a positive influence on enhancing

employees' risky decisions and ultimately make employees perform NISMs. Although curiosity and risk-taking behaviors are often encouraged in organizations as valuable factors to enhance creativity and productivity (Reio Jr & Wiswell, 2000; Yuan & Woodman, 2010), they can be considered as threats in the ISS.

Fourth, while the extant literature has discussed the role of information security awareness in changing belief, attitude, and intention to conform to ISSPs, this study empirically investigated the direct effect of information security awareness on employees' actual security behaviors. We also show that information security awareness has a positive impact on reducing NISMs since risky decisions can be regulated under high levels of security awareness, suggesting the strong effect of information security awareness and highlights the importance of this construct in the context of ISS.

Finally, our work contributes to understanding a relatively understudied concept of perceived work-overload in the context of ISS. Prior research has extensively investigated the effect of perceived work-overload on employees' performance, stress, turn over, and organizational commitment (Ayyagari et al., 2011; Moore, 2000), but to our best knowledge, this study is the first to empirically investigate the role of perceived work-overload in the context of an employee's NISMs. We show that high-level perception of work-overload will result in NISMs. Furthermore, it increases the probability of employees' unconscious risk-taking behaviors at the workplace to perform insecure behaviors. Recently, Greitzer, Strozer, Cohen, Bergey, et al. (2014) had proposed that work-overload could be a possible factor in enhancing unintentional security misbehaviors. In this research, we address this concern, and empirically show that perceived work-overload has a significant influence on employees' NISMs.

4.6.3 Practical Implications

The results of this study suggest important practical implications for information security management practice. Based on the results, we suggest that information security practitioners should consider new strategies regarding individual and organizational practices. First, our findings reveal a significant impact of personality traits on employees' ISSP compliance behavior, suggesting that individual differences cannot be taken for granted. Risk-taker employees with high impulsivity and curiosity are more likely to commit misbehavior and increase the risk of security threats in organizations. While risk-taking may be beneficial in some circumstances, this is not the case with information security. Assessment of employees' risk propensity and the level of their impulsive actions can be beneficial in order to take required counteractions to apply controls on these behaviors if necessary. Curiosity and risk-taking behaviors are encouraged to increase innovations and creativity for firm performance purposes (Reio Jr & Wiswell, 2000; Sauner-Leroy, 2004). Nonetheless, too much support of these behaviors can be threatening as they may change the culture and norm of organizations and influence employees' daily activities inherently, and consequently, risk-taking behaviors become a serious issue for information security.

Second, our findings provide evidence of a significant impact of perceived work-overload on insecure behaviors. The level of perceived workload might be different between employees. Therefore, job tasks should be allocated based on the skills and capabilities of employees. Otherwise, employees may prioritize to perform their primary job tasks rather than fulfill the information security requirements. Moreover, due to the high work-overload employees may feel stressed and fatigued and, as a result, neglect or pay less attention to information security activities. Employers should be aware that in as workload increase so do the propensity for employee to commit NISMs.

Third, the results of this study provide additional support for the strong influence of information security awareness. Since the lack of knowledge is rarely the fault of the user, organizations should

address this problem to ensure their employees have sufficient and up-to-date knowledge to secure organizational assets. Organizations should consider that the lack of security knowledge not only directly influences security misbehaviors but increases the likelihood of risk-taking behaviors in employees. Hence, information security awareness and training programs should be utilized regularly.

4.6.4 Limitations and Future Research

Although we believe this work makes several contributions to the ISS research, it has the following limitations. First, we used self-assessed scales to measure constructs of the proposed model. Especially in a case of NISMs, even though individuals were asked to respond whether they perform a particular behavior or not (instead of measuring intention), measuring actual violational behaviors in a field setting can upgrade the validity of the model. Moreover, we assumed that items of NISMs include both intentional and unintentional misbehaviors since under certain conditions, each behavior can be performed either consciously or unconsciously. Since existing scales do not capture unintentional misbehaviors, we note this as a limitation and call future researchers to develop such scales or design experiments that assess unintentional NISMs. Second, employees' risk-taking behaviors can be shaped within their organizations apart from a personality trait. Our sample includes employees across various industries and organizations with different levels of risk perception and risk culture. Treating all respondents the same can make a potential bias for the accuracy of the results. Third, in this study, the security risk associated with each NISM assumed to be equal, while individuals may perceive the potential risk of each differently. Future research could control the magnitude of insiders' risk perception associated with each misbehavior. Employees, even with a high-risk propensity, may behave differently based on the risk of security threats. Fourth, we limited the dimensions of the DST only to curiosity and impulsivity. Future research should consider other representatives, such as habitual behaviors for reflexive system or

self-regulatory factors (e.g., self-control, adaptability) for reflective system to examine their role in the context of ISSP compliance.

Finally, our post hoc analysis on the effect of demographic factors on NISM showed that age ($\beta = -0.22$, $p < 0.001$) and gender ($\beta = 0.13$, $p < 0.05$) are statistically significant determinants of NISMs. Future research should look at age and gender differences in risk-taking behaviors. Prior research indicates that females take fewer risks (Figner & Weber, 2011), but are less engaged in the best cybersecurity practices (Anwar et al., 2017). Examining gender differences in making risky decisions in the ISS context would advance our understanding of user behaviors.

4.7 Conclusion

Human error as the weakest link in information security remains a serious concern for organizations. This research enhanced our understanding of the impact of human factors on employees' non-compliance behaviors with ISSPs. Drawing on the DST, we distinguished intentional and unintentional NISMs and provided a theoretical framework to examine employees' conscious and unconscious risk-taking behavior on the likelihood of insecure behaviors. We found that employees with high risk-taking behavior are more likely to engage in unintentional/intentional NISMs. Also, impulsivity and curiosity are two individual factors that make employees more involved in unsecured practices via risky decisions with the exploitation of reflexive and reflective systems. Furthermore, we showed that when employees perceive high levels of work overload, they are more likely to make risky decisions and participate in insecure behaviors. In contrast, information security awareness can help employees to regulate their risky behaviors and less contribute to NISMs. This work supplemented behavioral research in the field of information security by demonstrating the role of human behaviors in organizations and providing insights into the potentiality of DST to describe both intentional and unintentional NISMs.

CHAPTER V

UNDERSTANDING UNINTENTIONAL INFORMATION SECURITY MISBEHAVIORS: A QUALITATIVE APPROACH

5.1 Introduction

Behavioral information Security (InfoSec) has drawn the attention of many scholars in recent decades since the increasing number of security incidents rooted in human behaviors have become a major concern of organizations (Ransbotham & Mitra, 2009; Warkentin & Willison, 2009). Despite past beliefs that external employees (outsiders) are the main security threats, most of the InfoSec violations occur within the organizations by insiders or internal employees (Baker et al., 2010; Ernst & Young, 2002). For this reason, behavioral InfoSec has taken account of many studies regarding computer abuse, unethical use, IS misuse, omissive behaviors, and InfoSec policy violations (Guo, 2013). The difference among these behaviors depends on the nature of intentions. Users intentionally violate InfoSec policies with either malicious intentions (e.g., sabotage or steal data) or non-malicious intentions (e.g., sharing the password with colleagues). Scholars extensively investigated insiders' intentional behaviors in terms of motives, objectives, mitigators, and outcomes (Bulgurcu et al., 2010; M. Siponen & A. Vance, 2010; Warkentin & Willison, 2009). However, statistical reports show that in most cases, insider threats are due to unintentional non-malicious InfoSec misbehaviors (NISMs) (Crossler et al., 2013; Identity Theft Resource Center, 2019) such as accidental disclosure of sensitive data via the internet. Insiders' unintentional NISMs are distinguishable from intentional NISMs, although both may have equally negative impacts

(Crossler et al., 2013; Greitzer, Strozer, Cohen, Bergey, et al., 2014). For example, a user may leave a PC unlocked volitionally because of avoiding logging-in frequently (non-malicious, intentional). The same user may unwillingly leave a PC unlocked because of running an immediate task (non-malicious, unintentional). However, both misbehaviors put the organization at risk of exposure. Based on previously applied theories in InfoSec studies, we argue that theoretical frameworks utilized to explain insiders' intentional NISMs are not appropriate in the context of unintentional NISM. Moreover, as per our knowledge, empirical studies investigating unintentional NISMs studies are relatively rare, and they are limited to provide definitions, examples, and introduce conceptual frameworks of possible predictors and consequences (Ayyagari, 2012; Crossler et al., 2013; Kraemer & Carayon, 2007). In a rare case, Greitzer, Strozer, Cohen, Moore, et al. (2014) examined insiders' unintentional responses to phishing attacks. However, we believe that unintentional NISMs are not confined only to phishing threats. Hence, there is a lack of understanding in individuals' unintentional NISMs, and further investigations are needed to generalize factors impacting unintentional NISMs.

To this end, we propose a qualitative approach by interviewing employees across different industries. Drawing on the behavioral InfoSec literature, we developed an interview protocol that we use to conduct semi-structured interviews to identify the most-occurred unintentional NISMs and to understand why users become involved in such unsecured behaviors unintentionally. In other words, we aim to understand the nature of the unintentional NISMs and to identify contributing factors of such misbehaviors rooted in individual or organizational factors. Particularly, we are going to answer the following research questions:

RQ1: What are the most common NISMs that employees commit unintentionally?

RQ2: What types of contextual (e.g., individual, organizational) factors cause unintentional NISMs? Why?

We believe that interviews will allow us to gain a broad range of perceptions about employees' unintentional NISMs at the workplace, and obtain a richer understanding of why individuals perpetrate unintentional NISMs. The results of our exploratory analysis will guide future researchers to develop theoretical models to find causal relationships between predictors and particular misbehaviors.

5.2 Literature review

Insiders are recognized to be the weakest link in InfoSec (rather than technical issues) and prevent organizations from achieving their InfoSec goals: confidentiality, integrity, availability, and accountability in the whole organization (Siponen, 2006; Willison & Warkentin, 2013). Insider threats arise from individuals who have the authorization to access to the information assets of the organization (Warkentin & Mutchler, 2014). To reduce the risk of insider threats, organizational strategies such as InfoSec policy and awareness programs are implemented (Siponen, 2000). However, the fact is that not all users comply exactly with security policies as prescribed (M. Siponen & A. Vance, 2010). Insiders' non-compliance behaviors with InfoSec policies are classified into three categories (Loch et al., 1992a; Willison & Warkentin, 2013): (1) intentional, malicious computer abuse; (2) volitional (but not malicious) non-compliance; and (3) passive, non-volitional non-compliance.

The first category belongs to individuals who intentionally with malicious intentions threaten organizations' security through deliberate actions (Liang et al., 2016). Examples of malicious behaviors are sabotage, data theft or corruption, fraud, or any deliberate policy violation, which are known as cybercrime (Warkentin & Mutchler, 2014). Potential malicious insiders' characteristics or causes are personality problems, mental health disorders, personal or work-related events (e.g., sanctions or loss of family member), emotional issues, social conflict, financial status, and other elements indicated by Liang et al. (2016). Moreover, dark triad personality traits (e.g., lack of

impulse control), motive, computer dependency, ethical flexibility, capability, and reduced loyalty impact insiders' malicious intent (Maasberg, Warren, & Beebe, 2015; Shaw, Post, & Ruby, 1999).

The second category explains insiders with non-malicious intentions who involve in unsecured volitional behaviors such as writing down a password or sharing it with a colleague, leaving a PC unlocked, installing unauthorized software, using personal devices for organizational work, and delayed backups. Scholars define insiders' intentional NISMs as behaviors that are done knowingly with conscious decisions against the organizational security policies with no malicious intent to cause destruction (K. H. Guo, Y. Yuan, N. P. Archer, & C. E. J. J. o. m. i. s. Connelly, 2011b). Non-malicious insiders violate policies voluntarily for their benefits like saving time and effort (Greitzer, Strozer, Cohen, Moore, et al., 2014; Guo et al., 2011b). The main motivations of these behaviors are utilitarian outcomes, normative outcomes, and self-identity outcomes, as determined by Guo et al. (2011b). These violations can be addressed and explained through neutralization, rationalization, cost-benefit analysis, persuasion, deterrence, or any other behavioral control (M. Siponen & A. Vance, 2010; Warkentin & Mutchler, 2014).

Finally, third class refers to unintentional insider threats which arise from users' NISMs who have authorized access to the organizational assets but inadvertently without harmful intentions violate security policies (Ayyagari, 2012; Greitzer, Strozer, Cohen, Bergey, et al., 2014). Human errors with no awareness of a misdeed such as accidental modification of software, corruption of data by a programming error, accidental clicks on phishing emails, forget to lock the PC, sending sensitive data to the wrong recipient, and accidental data exposure are some examples of unintentional NISMs. This type of threat is often used interchangeably with non-malicious threats, while they are two different concepts (Guo et al., 2011b). In both cases, insiders do not have harmful intentions or ill will motivations, but the main difference is that an unintentional insider breaks the rule unwillingly, and through an honest mistake, whereas an intentional insider performs NISMs by his/her own will and break the rules on purpose. One can infer that insiders with unintentional

NISMs are not aware of their actions in terms of how, when, and what. They may realize their misbehaviors after the incidents. Hence, they do not expect any beneficial outcomes as opposed to non-malicious insiders who expect some desirable outcomes such as quicker task completion (Guo et al., 2011b). Unintentional NISMs emerge from negligent users who are not aware they expose their organizations to security risk (e.g., fail to lock down a PC due to running immediate task), but intentional NISMs resulted from conscious decisions to violate security rules (e.g., fail to lock down a PC due to not log-in frequently).

Although prior studies provided precious insights on employees' security-related behaviors, we argue that most behavioral InfoSec studies provide little context concerning unintentional NISMs. First, each type of insider threat has a different nature in terms of intention, motivations, influencers, and perceived outcomes, suggesting that the findings of each type of misbehaviors are exclusive and cannot be fully generalized to other types of violations. For instance, although the concept of non-malicious intentional and unintentional misbehaviors may be blurred because of having no harmful intentions, they possess different rationales and casual factors. The former are rule-breakers with known reasons, but the latter involves those who do not know how, when, and under what circumstance they threatened security or broke the rules.

Second, scholars utilized various theories to provide deep understating of individual's NISMs such as the theory of planned behavior (Bulgurcu et al., 2010), deterrence theory (Straub Jr, 1990), motivation-protection theory (Ifinedo, 2012), neutralization theory (M. Siponen & A. Vance, 2010), and rational choice theory (Li et al., 2010). These theories, mainly employed to explain employees' cognitive and intentional NISMs, and they might not be appropriate in the context of unintentional NISMs. They attempted to explain the reasons for the omission of secure behaviors of people who fail to protect their systems, albeit they know how to do so (Workman et al., 2008).

Third, to the best of our knowledge, the number of studies explaining unintentional NISMs is limited. There are a few conceptual studies devoted to identifying possible contributed factors such as organizational or human-related factors. According to Greitzer, Strozer, Cohen, Bergey, et al. (2014), possible organizational factors may include an unfair work setting (e.g., interruptions), weak management systems (e.g., multitasking), and inadequate InfoSec training practices. Taylor (2006) found that management's misperception of security risk gives rise to employees' unintentional NISMs. As human factors, personality traits (e.g., risk propensity, curiosity) and health/psychological status (e.g., using drugs, stress and anxiety, sleepiness) may be potential reasons for NISMs (Ayyagari, 2012; Meek, Clark, & Solana, 1989). In some cases, scholars examined reasons that why employees respond to phishing emails like as risk propensity, curiosity, or high email loads (Greitzer, Strozer, Cohen, Moore, et al., 2014; Moody et al., 2017; Vishwanath, Herath, Chen, Wang, & Rao, 2011). Since the scope of NISMs are not limited only to phishing threats (i.e., they include but not limited to password sharing, password write down, failure to log off, and using personal devices for work purposes (Guo et al., 2011b)), we believe further research is needed to study users' unintentional NISMs to generalize the findings. Furthermore, the increasing number of unintentional InfoSec incidents (Identity Theft Resource Center, 2019) provides additional motivations to conduct empirical studies. To address the aforementioned gaps in the literature, we next describe a qualitative approach to explore and explain factors contributed to unintentional NISMs.

5.3 Research Method: Data Collection and Data Analysis

The research context to investigate factors that impact unintentional NISMs lacks in providing an in-depth understanding of the InfoSec literature. Thus, we will conduct an exploratory research approach to interview employees to obtain their perceptions about unintentional NISMs as they are the weakest InfoSec at the workplace. We followed Mason (2017) approach to design a semi-structured interview protocol using open-ended questions, starting from broad questions, and then

dividing them into mini questions. Our interview questions consisted of demographics asking about their background, organizations' security training practices, work environment, and managerial controls (e.g., monitoring). Then it followed by questions relative to common InfoSec behaviors adapted by the literature, including device securement, password behaviors, clean desk, online behaviors, software updating, and remote access (Egelman & Peer, 2015; Guo et al., 2011b). In order to gain a rich understanding of NISMs' leading factors, we designed questions in a way that to derive employees' perceptions of why they committed a particular NISM. We asked whether they were conscious or unconscious of potential vulnerabilities while the misbehavior occurred and what was the possible factors that caused those misbehaviors. Table 5.1 presents our survey questions.

We have started to collect data from a sample of informants, including employees in different positions and an InfoSec management team (Chief information security officer, security analyst) of a relatively large company (fuel service company ~ 22k employees). Once data are collected, we will analyze data following open, axial, and selective coding processes in order to find major themes and constructs in explaining unintentional NISMs (Strauss & Corbin, 1990). We will use the causal mapping technique to investigate the patterns and magnitude of the causality between identified factors and certain unintentional NISM (see figure 5.1). Causal mapping is a word-arrow diagram that indicates how one idea or action leads to another (Bryson, Ackermann, Eden, & Finn, 2004). It usually includes map-level, construct-level, and between-constructs-level analysis to calculate density, centrality, and reachability among constructs (Ghobadi & Mathiassen, 2016).

5.4 Preliminary Results

After the analysis of a few qualitative data, an initial set of codes were determined. So far, the results showed that some organizational and human factors provide favorable situations for insiders to perform both intentional and unintentional NISMs.

Table 5.1 Interview protocol

Demographics:

Gender, major, age, industry, company size, full/part time, daily working hours, daily computer usage

Interview questions:

What is/was your job position?
How many years of experience do you have?
Do you feel overloaded by the level of work you are asked to perofrm?
On a scale of 1-5 (1 is very low, 5 is very high), how distracting is your work environment? Explain.

Are you aware of your company's security policies?
On a scale of 1-5 (1 is very low, 5 is very high), how do you rate your level of information security awareness?
Were you trained in IS security practices at work?
What was the training like? Please explain.
Were you trained during your orientation? Since orientation?

Are you being monitored or observed during work that you know of?

What best information security behaviors have you ever performed? Mark all that apply.

Were you conscious of potential vulnerabilities when you were committing those misbehaviors?
1- Intentional
   i. What do you think were the possible factors that caused those misbehaviors (e.g., careless, no fear, risk-taker, no policy, lack of monitoring, had to get another task done, etc.)?
   ii. Any benefits that you could get by committing those misbehaviors?
2- Unintentional
   i. What do you think were the possible factors that caused those misbehaviors? What was the reason of the accident? (e.g., being distracted, ….)

Did you report your misbehavior to your company? Or shared with your colleague(s)? Why?

Did/do you continue to commit such misbehaviors?

Have you ever seen your colleagues deviate from security policies? Any idea why?

Information Security Behaviors	**Check all that apply**	**Intent (Intentionally/Unintentionally)**
Device Securement		
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.		
I use a password/passcode to unlock my laptop or tablet.		
I lock my computer screen when I step away from it.		
I use a PIN or passcode to unlock my mobile phone.		
I lock the door of my office when I leave the room.		
Password Behaviors		
I change my passwords even if I don't have to.		
I use different passwords for different accounts that I have.		
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.		
I include special characters in my password even if it's not required.		

I don't share passwords with friends and colleagues.		
I don't use or create simple passwords (e.g. family name and date of birth).		
Clean Desk		
I don't write down my username and password on stickers and put them on my desk or attach to the computer.		
Online Behaviors (Websites)		
I don't open a link without first verifying where it goes.		
I don't click on links that I receive without checking the source of the email they came in.		
When browsing websites, I don't click on links, before mouseover-ing them to see where they go.		
I don't open links contained in an email even from a trusted friend or work colleague without verifying where it leads.		
I don't visit a website based on its look and feel, rather I look at the URL bar.		
I don't submit information to websites without checking their security information/certification.		
Software Installation/Updating		
I don't download applications from an unknown source.		
I don't download data and material from websites on my work computer without checking its authenticity.		
When I'm prompted to reboot my computer to initiate a software update (the first time), I don't postpone it.		
Remote/Network Access		
I don't bring my own USB to work in order to transfer data onto it even if it is not against the company's policy.		
I don't use free public Wi-Fi for work purposes.		
I don't use online storage systems to exchange and keep personal or sensitive information. (e.g., Dropbox, Google Drive)		
I don't store company information on my personal electronic device. (e.g., smartphone/laptop, USB) if it is not against my company's policy.		

Security management practices. Although InfoSec training was found to impact employees' compliance behaviors (Bulgurcu et al., 2010), a lack of managerial practices to follow up and monitor employees to ensure that they comply can be a potential security risk. We asked for managerial practices like being observed at work. The response was "Besides the initial presentation (training) of not to do, I guess if there were no reinforcement, I would never have created those habits to ensure security."

Risk propensity. It has been mentioned by some scholars that there might be a relationship between risk-taking behaviors and unintentional NISMs (Bureau, 2013). Our data provided support for this relationship. We asked about their online behavior like browsing a website. The response was: "I don't look at the URL and usually feel the website. I feel like I have a great radar so far, I was lucky, I guess". We anticipate more factors related to individuals and organizations that link to unintentional NISMs. We expect that each of these factors includes sub-constructs that some may have a stronger effect than others on overall unintentional NISMs.

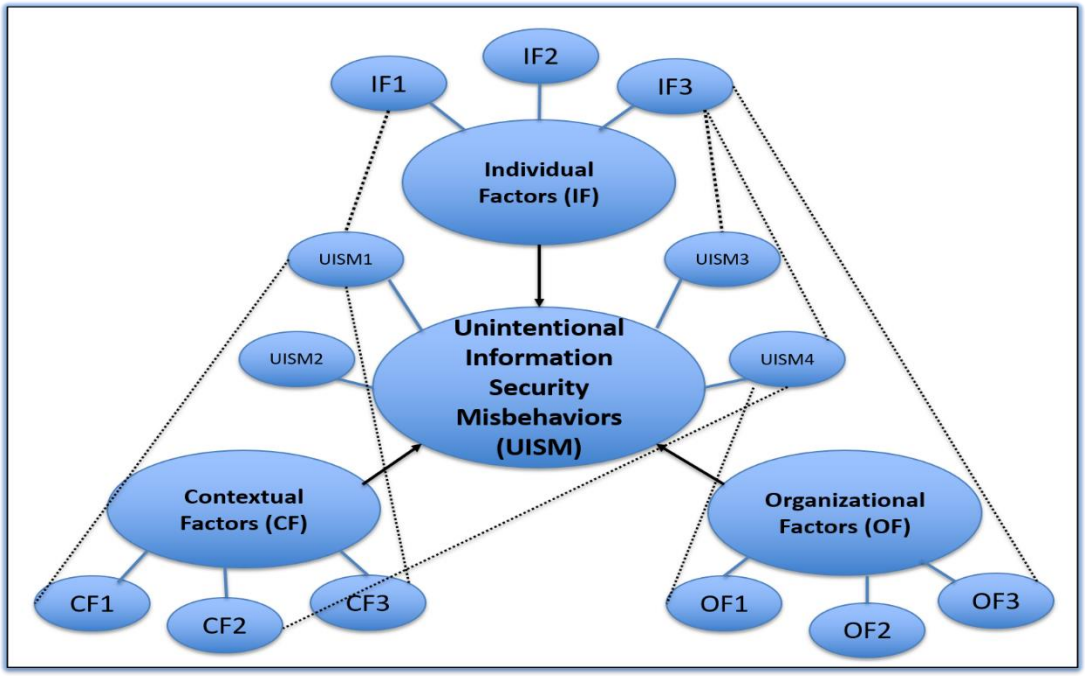

Figure 5.1 Expected causal map

5.5 Conclusion

In order to gain a deep understanding of insiders' unintentional NISMs, an exploratory qualitative study is conducted to determine factors influencing unintentional NISMs. While previous

researchers have provided the conceptual studies to define and propose possible factors, this empirical study will shed light on behavioral InfoSec literature and contributes to the context of NISMs by identifying significant factors, either organizational or individual, that lead employees to commit unintentional NISMs. The results of this study can (1) provide insights to InfoSec management in order to modify/implement new strategies in the workplace to reduce the likelihood of performing unintentional NISMs, and (2) motivate future researchers to propose experimental designs and quantitative studies, to conduct observational research, and to develop theoretical models in order to assess causal relationships between antecedents and NISMs.

REFERENCES

Abed, J., Dhillon, G., & Ozkan, S. (2016). *Investigating continuous security compliance behavior: Insights from information systems continuance model.* Paper presented at the Twenty-second Americas Conference on Information Systems.

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32*(3), 183-196.

Abu-Musa, A. A. (2006). Perceived security threats of computerized accounting information systems in the Egyptian banking industry. *Journal of Information Systems, 20*(1), 187-203.

AbuAlRub, R. F. (2004). Job stress, job performance, and social support among hospital nurses. *Journal of Nursing Scholarship, 36*(1), 73-78.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology, 30*(1), 47-88.

Ahuja, M. K., Chudoba, K. M., Kacmar, C. J., McKnight, D. H., & George, J. F. (2007). IT Road Warriors: Balancing Work-Family Conflict, Job Autonomy, and Work Overload to Mitigate Turnover Intentions. *MIS Quarterly, 31*(1), 1-17. doi:10.2307/25148778

Aiken, L. S., West, S. G., & Reno, R. R. (1991). *Multiple regression: Testing and interpreting interactions*: Sage.

Aivazpour, Z., & Rao, V. S. (2018). *Impulsivity and Risky Cybersecurity Behaviors: A Replication*. Paper presented at the Twenty-fourth Americas Conference on Information Systems, New Orleans

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

Anderson, J. C., & Gerbing, D. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443.

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research, 12*(1), 1-11.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security, 8*(2), 33-56.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: technological antecedents and implications. *MIS Quarterly, 35*(4), 831-858.

Badie, N., & Lashkari, A. H. (2012). A new evaluation criteria for effective security awareness in computer risk management based on AHP. *Journal of Basic and Applied Scientific Research, 2*(9), 9331-9347.

Baker, W., Goudie, M., Hutton, A., Hylender, C., Niemantsverdriet, J., Novak, C., . . . Sartin, B. (2010). Verizon 2010 Data Breach Investigations Report. Verizon Business. In.

Barclay, D., Higgins, C., & Thompson, R. (1995). *The partial least squares (PLS) approach to casual modeling: Personal computer adoption and use as an illustration*. Berlin: Walter de Gruyter.

Barclay, D., Higgins, C., & Thompson, R. (1995). *The partial least squares (PLS) approach to casual modeling: personal computer adoption ans use as an Illustration*: Walter de Gruyter.

Bargh, J. A. (2014). *The four horsemen of automaticity: Awareness, intention, efficiency, and control in social cognition* (Vol. 1): Psychology Press.

Baron, R. M., & Kenny, D. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173.

Barringer, B. R., & Bluedorn, A. C. (1999). The relationship between corporate entrepreneurship and strategic management. *Strategic Management Journal, 20*(5), 421-444.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17): Sage.
Becker, J.-M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: guidelines for using reflective-formative type models. *Long Range Planning, 45*(5-6), 359-394.
Beehr, T. (1998). An organizational psychology meta-model of occupational stress. In *Theories of organizational stress* (pp. 6-27): Oxford University Press.
Beehr, T. A., Jex, S. M., Stacy, B. A., & Murray, M. A. (2000). Work stressors and coworker support as predictors of individual strain and job performance. *Journal of Organizational Behavior, 21*(4), 391-405.
Bellika, J. G., Makhlysheva, A., & Bakkevoll, P. A. (2018). *A significant increase in the risk for exposure of health information in the United States: result from analysing the US data breach registry.* Paper presented at the Proceedings from The 15th Scandinavian Conference on Health Informatics, Kristiansand, Norway.
Bennett, P. (2010). *Risk communication and public health*: Oxford University Press.
Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*(3), 253-264.
Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: an empirical investigation. *MIS Quarterly, 24*(1), 169-196.
Bhattacherjee, A., & Hikmet, N. (2008). Reconceptualizing organizational support and its effect on information technology usage: Evidence from the health care sector. *Journal of Computer Information Systems, 48*(4), 69-76.
Biddle, B. J. (1986). Recent developments in role theory. *Annual Review of Sociology, 12*(1), 67-92.
Biros, D., Daly, M., & Gunsch, G. (2004). Task Load and Automation Use in an Uncertain Environment. *Group Decision & Negotiation, 13*(2).
Biros, D. P., Daly, M., & Gunsch. (2004). The Influence of Task Load and Automation Trust on Deception Detection. *Group Decision Negotiation, 13*(2), 173-189. doi:10.1023/b:Grup.0000021840.85686.57
Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64-68.
Božić, G. (2012). *The role of a stress model in the development of information security culture.* Paper presented at the 2012 Proceedings of the 35th International Convention MIPRO.
Brady, J. W. (2010). *An investigation of factors that affect HIPAA security compliance in academic medical centers.* (Doctor of Philosophy in Information Systems (DISS)), Nova Southeastern University,
Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems, 25*(4), 364-390.
Brod, C. (1984). *Technostress: The human cost of the computer revolution*: Addison Wesley Publishing Company.
Bromiley, P., & Curley, S. P. (1992). *Individual differences in risk taking*: John Wiley & Sons.
Brown, T. A. (2015). *Confirmatory factor analysis for applied research*: Guilford Publications.
Brynjolfsson, E., & Hitt, L. M. (2003). Computing productivity: Firm-level evidence. *Review of Economics and Statistics, 85*(4), 793-808.
Bryson, J. M., Ackermann, F., Eden, C., & Finn, C. B. (2004). *Visible thinking: Unlocking causal mapping for practical business results*: John Wiley & Sons.
Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.
Bureau, F. I. P. (2013). Unintentional Insider Threats: A Foundational Study. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf
Burke, M. J., Brief, A. P., & George, J. M. (1993). The role of negative affectivity in understanding relations between self-reports of stressors and strains: a comment on the applied psychology literature. *Journal of Applied Psychology, 78*(3), 402.
Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly, 30*(2), 211-224.
Byrne, B. M. (2013). *Structural equation modeling with Mplus: Basic concepts, applications, and programming*: Routledge.
Califf, C. B., Sarker, S., & Sarker, S. (2020). The Bright and Dark Sides of Technostress: A Mixed-Methods Study Involving Healthcare IT. *MIS Quarterly, 44*(2).
Campbell, S. (2005). Determining overall risk. *Journal of Risk Research, 8*(7-8), 569-581.

Cao, X., Masood, A., Luqman, A., & Ali, A. (2018). Excessive use of mobile social networking sites and poor academic performance: Antecedents and consequences from stressor-strain-outcome perspective. *Computers in Human Behavior, 85*, 163-174.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. J. C. o. t. A. f. I. S. (2004). Economics of ITSecurity Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems, 14*(1), 3.

Chang, C., Gardiner, J., Houang, R. T., & Yu, Y.-L. (2020). *Comparing Multiple Statistical Software for Multiple-Indicator, Multiple-Cause Modeling: An Application of Gender Disparity in Adult Cognitive Functioning Using MIDUS II Dataset*. (PREPRINT (Version 4)). Researchsquare.

Chang, S.-H., Hsu, H.-M., Li, Y., & Hsu, J. S.-C. (2018). *The Influence of Information Security Stress on Security Policy Compliance: A Protection Motivation Theory Perspective.* Paper presented at the PACIS.

Chen, A., & Karahanna, E. (2018). Life interrupted: The effects of technology-mediated work interruptions on work and nonwork outcomes. *MIS Quarterly, 42*(4), 1023-1042.

Chen, P. Y., & Spector, P. E. (1992). Relationships of work stressors with aggression, withdrawal, theft and substance use: An exploratory study. *Journal of Occupational & Organizational Psychology, 65*(3), 177-184.

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.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1).

Choi, C. H., Kim, T. T., Lee, G., & Lee, S. K. (2014). Testing the stressor–strain–outcome model of customer-related social stressors in predicting emotional exhaustion, customer orientation and service recovery performance. *International Journal of Hospitality Management, 36*, 272-285.

Cohen, S., Janicki-Deverts, D., & Miller, G. E. (2007). Psychological stress and disease. *Journal of Americam Medical Association, 298*(14), 1685-1687.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology, 92*(4), 909.

Cooper, C. L., Cooper, C. P., Dewe, P. J., O'Driscoll, M. P., & O'Driscoll, M. P. (2001). *Organizational stress: A review and critique of theory, research, and applications*. CA: Sage.

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., & Huettel, S. A. (2014). An Abbreviated Impulsiveness Scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version 11. *Archives of Scientific Psychology, 2*(1), 1.

Coverman, S. (1989). Role overload, role conflict, and stress: Addressing consequences of multiple role demands. *Social forces, 67*(4), 965-982.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849-1858.

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525-554.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

CSI. (2010). CSI Computer Crime and Security Survey. In *Computer Security Institute*.

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*(6), 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*(2), 285-318.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

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

D'Arcy, J. P. (2005). *Security countermeasures and their impact on information systems misuse: A deterrence perspective.* (Doctor of Philosophy), Temple University,

D'Arcy, J., Gupta, A., Tarafdar, M., & Turel, O. (2014). Reflecting on the "dark side" of information technology use. *Communications of the Association for Information Systems, 35*(1), 5.
D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization. *Information & Management, 56*(7), 103151.
Dewett, T. (2006). Exploring the role of risk in employee creativity. *The Journal of Creative Behavior, 40*(1), 27-45.
Dewett, T. (2007). Linking intrinsic motivation, risk taking, and employee creativity in an R&D environment. *R & D Management, 37*(3), 197-208.
Donalds, C. (2015). *Cybersecurity policy compliance: an empirical study of Jamaican government agencies.* Paper presented at the SIG GlobDev Pre-ECIS Workshop, Munster, Germany.
Edwards, J. R. (1996). An examination of competing versions of the person-environment fit approach to stress. *Academy of Management Journal, 39*(2), 292-339.
Egelman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (sebis).* Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.
Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived organizational support. *Journal of Applied Psychology, 71*(3), 500.
El Halabieh, R., Beaudry, A., & Tamblyn, R. (2017). *Impacts of stress, satisfaction and behavioral intention on continued usage: evidence from physicians transitioning to a new drug management system.* Paper presented at the Proceedings of the 50th Hawaii International Conference on System Sciences.
Eppler, M. J., & Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. *The Information Society, 20*(5), 325-344.
Ernst, Y. L., & Young, X. (2002). Global information security survey. In *UK: Presentation Services*.
Evans, J. S. B. (2003). In two minds: dual-process accounts of reasoning. *Trends in Cognitive Sciences, 7*(10), 454-459.
Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*: University of Akron Press.
Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. *Information Systems Frontiers, 15*(1), 5-15.
Farrell, A. M., & Rudd, J. M. (2009). *Factor analysis and discriminant validity: A brief review of some practical issues.* Paper presented at the ANZMAC.
Figner, B., & Weber, E. U. (2011). Who takes risks when and why? Determinants of risk taking. *Current Directions in Psychological Science, 20*(4), 211-216.
Fischer, T., Pehböck, A., & Riedl, R. (2019). *Is the technostress creators inventory still an up-to-date measurement instrument? Results of a large-scale interview study*. Paper presented at the 14th International Conference on Wirtschaftsinformatik.
Fischer, T., & Riedl, R. (2015). *Theorizing Technostress in Organizations: A Cybernetic Approach.* Paper presented at the Wirtschaftsinformatik.
Fisher, D. M., Kerr, A. J., & Cunningham, S. (2019). Examining the moderating effect of mindfulness on the relationship between job stressors and strain outcomes. *International Journal of Stress Management, 26*(1), 78.
Florkowski, G. W. (2019). HR technologies and HR-staff technostress: an unavoidable or combatable effect? *Employee Relations: The International Journal, 41*(5).
Forester, T., & Morrison, P. (1990). Computer unreliability and social vulnerability. *Futures, 22*(5), 462-474.
Forman, C., King, J. L., & Lyytinen, K. (2014). Special section introduction—information, technology, and the changing nature of work. *Information Systems Research, 25*(4), 789-795.
Fornell, C., & Larcker, D. F. (1981a). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39-50.
Fornell, C., & Larcker, D. F. (1981b). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.
Frese, M. (1999). Social support as a moderator of the relationship between work stressors and psychological dysfunctioning: A longitudinal study with objective measures. *Journal of occupational health psychology, 4*(3), 179.

Galluch, P. S., Grover, V., & Thatcher, J. B. (2015). Interrupting the workplace: Examining stressors in an information technology context. *Journal of the Association for Information Systems, 16*(1), 2.
Gaudioso, F., Turel, O., & Galimberti, C. (2017). The mediating roles of strain facets and coping strategies in translating techno-stressors into adverse job outcomes. *Computers in Human Behavior, 69*, 189-196.
Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(1), 7.
Ghobadi, S., & Mathiassen, L. (2016). Perceived barriers to effective knowledge sharing in agile software teams. *Information Systems Journal, 26*(2), 95-125.
Gloster, R. (2018). Seven ways online platrforms have changed how we work. Retrieved from https://www.employment-studies.co.uk/news/seven-ways-online-platforms-have-changed-how-we-work
Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358.
Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., & Mundie, D. (2014). *Unintentional insider threat: contributing factors, observables, and mitigation strategies.* Paper presented at the 2014 47th Hawaii International Conference on System Sciences.
Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). *Analysis of unintentional insider threats deriving from social engineering exploits.* Paper presented at the Security and Privacy Workshops (SPW), 2014 IEEE.
Grewal, R., Cote, J. A., & Baumgartner, H. (2004). Multicollinearity and measurement error in structural equation models: Implications for theory testing. *Marketing Science, 23*(4), 519-529.
Grover, V., Teng, J. T., & Fiedler, K. D. (2002). Investigating the role of information technology in building buyer-supplier relationships. *Journal of the Association for Information Systems, 3*(1), 7.
Guimaraes, T., & Igbaria, M. (1992). Determinants of turnover intentions: Comparing IC and IS personnel. *Information Systems Research, 3*(3), 273-303.
Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242-251.
Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011a). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.
Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. J. J. o. m. i. s. (2011b). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.
Hadlington, L. J. H. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346.
Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (Seventh Edition ed.): Pearson Prentice Hall.
Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (1998). *Multivariate data analysis* (Vol. 5). Prentice hall Upper Saddle River, NJ: Pearson.
Henle, C. A. (2005). Predicting workplace deviance from the interaction between organizational justice and personality. *Journal of Managerial Issues*, 247-263.
Henle, C. A., & Blanchard, A. L. (2008). The interaction of work stressors and organizational sanctions on cyberloafing. *Journal of Managerial Issues*, 383-400.
Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.
Hinkin, T. R., Tracey, J. B., & Enz, C. A. (1997). Scale construction: Developing reliable and valid measurement instruments. *Journal of Hospitality &Tourism Research, 21*(1), 100-120.
Ho-Jin, P., & Cho, J.-S. (2016). The influence of information security technostress on the job satisfaction of employees. *Journal of Business Retail Management Research, 11*(1).
Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282-300.
Hudiburg, R. A. (1995). Psychology of computer use: XXXIV. The Computer Hassles Scale: Subscales, norms, and reliability. *Psychological Reports, 77*(3), 779-782.
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.

IBM. (2019). IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years. Retrieved from https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years#assets_all

IBM Global technology Service. (2014). IBM Security Services 2014 Cyber Security Intelligence Index. Retrieved from https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

Identity Theft Resource Center. (2019). 2018 End of year Data breach Report. Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf

IDG Research. (2018). 2018 U.S. State of Cybercrime. Retrieved from https://www.idg.com/tools-for-marketers/2018-u-s-state-of-cybercrime/

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

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79.

Igbaria, M., & Siegel, S. R. (1992). The reasons for turnover of information systems personnel. *Information & Management*, *23*(6), 321-330.

Ioannou, A., & Papazafeiropoulou, A. (2017). *Using IT mindfulness to mitigate the negative consequences of technostress*. Paper presented at the Twenty-third Americas Conference on Information Systems.

Islam, N., Mavengere, N., Ahlfors, U.-R., Ruohonen, M., Serenko, A., & Palvia, P. (2018). *A Stress-Strain-Outcome Model of Job Satisfaction: The Moderating Role of Professional Self-efficacy*. Paper presented at the Twenty-fourth Americas Conference on Information Systems.

J. Clement. (2019). *Cyber crime: number of breaches and records exposed 2005-2018*. 5 Aug. Retrieved from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed

J. Clement. (2020). *Cyber crime: number of breaches and records exposed 2005-2019*. 5 Aug. Retrieved from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed

Jawahar, I., Stone, T. H., & Kisamore, J. L. (2007). Role conflict and burnout: The direct and moderating effects of political skill and perceived organizational support on burnout dimensions. *International Journal of Stress Management*, *14*(2), 142.

Jena, R. (2015). Technostress in ICT enabled collaborative learning environment: An empirical study among Indian academician. *Computers in Human Behavior*, *51*, 1116-1123.

Kahn, R. L., Wolfe, D. M., Quinn, R. P., Snoek, J. D., & Rosenthal, R. A. (1964). *Organizational stress: Studies in role conflict and ambiguity*: John Wiley.

Kanter, R. M. (1968). Commitment and social organization: A study of commitment mechanisms in utopian communities. *American Sociological Review*, 499-517.

Kaplan, D. (1994). Estimator conditioning diagnostics for covariance structure models. *Sociological methods & Research*, *23*(2), 200-229.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11-27.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. *Information Systems Research*, *30*(2), 687-704.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 3.

Kashdan, T. B., Elhai, J. D., & Breen, W. E. (2008). Social anxiety and disinhibition: an analysis of curiosity and social rank appraisals, approach–avoidance conflicts, and disruptive risk-taking behavior. *Journal of Anxiety Disorders*, *22*(6), 925-939.

Kashdan, T. B., Rose, P., & Fincham, F. D. (2004). Curiosity and exploration: Facilitating positive subjective experiences and personal growth opportunities. *Journal of Personality Assessment*, *82*(3), 291-305.

Katz, D., & Kahn, R. L. (1978). *The social psychology of organizations* (Vol. 2): Wiley New York.

Keenan, A., & Newton, T. (1985). Stressful events, stressors and psychological strains in young professional engineers. *Journal of Organizational Behavior*, *6*(2), 151-156.

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2020). DATA BREACH MANAGEMENT: AN INTEGRATED RISK MODEL. *Information & Management*, 103392.

Kidd, C., & Hayden, B. Y. (2015). The psychology and neuroscience of curiosity. *Neuron, 88*(3), 449-460.
Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564.
Kim, W. C., & Mauborgne, R. A. (1996). Procedural justice and managers' in-role and extra-role behavior: The case of the multinational. *Management Science, 42*(4), 499-515.
King, R. C., & Sethi, V. (1997). The moderating effect of organizational commitment on burnout in information systems professionals. *European Journal of Information Systems, 6*(2), 86-96.
Kinman, G., & Jones, F. (2005). Lay representations of workplace stress: What do people really mean when they say they are stressed? *Work & Stress, 19*(2), 101-120.
Kline, R. B. (2015). *Principles and practice of structural equation modeling*: Guilford Publications.
Koohang, A., Nord, J. H., Sandoval, Z. V., & Paliszkiewicz, J. (2020). Reliability, Validity, and Strength of a Unified Model for Information Security Policy Compliance. *Journal of Computer Information Systems*, 1-9.
Kraemer, S., & Carayon, P. J. A. e. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics, 38*(2), 143-154.
Lambert, E. G., Hogan, N. L., Paoline, E. A., & Clarke, A. (2005). The impact of role stressors on job stress, job satisfaction, and organizational commitment among private prison staff. *Security Journal, 18*(4), 33-50.
Lazarus, R. S. (1993). From psychological stress to the emotions: A history of changing outlooks. *Annual review of psychology, 44*(1), 1-22.
Lei, C. F., & Ngai, E. W. (2014). *The double-edged nature of technostress on work performance: A research model and research agenda*. Paper presented at the Thirty Fifth International Conference on Information Systems.
Leiter, M. P., & Schaufeli, W. B. (1996). Consistency of the burnout construct across occupations. *Anxiety, Stress, and Coping, 9*(3), 229-243.
Leonard, L. N., & Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association for Information Systems, 1*(1), 12.
Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 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.
Liang, H., & Xue, Y. (2009a). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90.
Liang, H., & Xue, Y. (2009b). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*, 71-90.
Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems, 33*(2), 361-392.
Lieberman, M. D. (2007). Social cognitive neuroscience: a review of core processes. *Annual Review Psychology, 58*, 259-289.
Liu, Z., Wang, X., Min, Q., & Li, W. (2019). The effect of role conflict on self-disclosure in social network sites: An integrated perspective of boundary regulation and dual process model. *Information Systems Journal, 29*(2), 279-316.
Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992a). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.
Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992b). Threats to information systems: today's reality, yesterday's understanding. *MIS quarterly*, 173-186.
Loewenstein, G. (1994). The psychology of curiosity: A review and reinterpretation. *Psychological Bulletin, 116*(1), 75.
Low, G. S., Cravens, D. W., Grant, K., & Moncrief, W. C. (2001). Antecedents and consequences of salesperson burnout. *European Journal of Marketing*.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal, 25*(5), 433-463.
Lukacs, E., Negoescu, G., & David, S. (2009). Employees Misbehaviour: Formes, Causes and What Management Should do to Handle With. *Economics and Applied Informatics*.
Maasberg, M., Warren, J., & Beebe, N. L. (2015). *The dark side of the insider: detecting the insider threat through examination of dark triad personality traits.* Paper presented at the System Sciences (HICSS), 2015 48th Hawaii International Conference on.
MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *Journal of Applied Psychology, 90*(4), 710.
MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293-334.
Mahmmod Sher-Jan. (2018). Full disclosure: Benchmarking data reveals the human error in privacy incidents. Retrieved from https://www.radarfirst.com/blog/human-error-in-privacy-incidents/
Maier, C., Laumer, S., Weinert, C., & Weitzel, T. (2015). The effects of technostress and switching stress on discontinued use of social networking services: a study of Facebook use. *Information Systems Journal, 25*(3), 275-308.
Maier, C., Laumer, S., Wirth, J., & Weitzel, T. (2019). Technostress and the hierarchical levels of personality: a two-wave study with multiple data samples. *European Journal of Information Systems, 28*(5), 496-522.
Marchiori, D. M., Mainardes, E. W., & Rodrigues, R. G. (2019). Do Individual Characteristics Influence the Types of Technostress Reported by Workers? *International Journal of Human–Computer Interaction, 35*(3), 218-230.
Mason, J. (2017). *Qualitative researching*: Sage.
McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information & Computer Security*.
McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.
McGhee, R. L., Ehrler, D. J., Buckhalt, J. A., & Phillips, C. (2012). The relation between five-factor personality traits and risk-taking behavior in preadolescents. *Psychology, 3*(8), 558.
Meek, P. S., Clark, H. W., & Solana, V. L. (1989). Neurocognitive impairment: The unrecognized component of dual diagnosis in substance abuse treatment. *Journal of Psychoactive Drugs, 21*(2), 153-160.
Metcalfe, J., & Mischel, W. (1999). A hot/cool-system analysis of delay of gratification: dynamics of willpower. *Psychological Review, 106*(1), 3.
Mishra, S., & Lalumière, M. L. (2011). Individual differences in risk-propensity: Associations between personality and behavioral measures of risk. *Personality and Individual Differences, 50*(6), 869-873.
Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems, 26*(6), 564-584.
Moore, J. E. (2000). One road to turnover: An examination of work exhaustion in technology professionals. *MIS Quarterly, 24*(1), 141-168.
Mowday, R. T., Porter, L. W., & Steers, R. M. (1982). *Employee—organization linkages: The psychology of commitment, absenteeism, and turnover*: Academic press.
Mukherjee, K. (2010). A dual system model of preferences under risk. *Psychological Review, 117*(1), 243.
Mussel, P., Spengler, M., Litman, J. A., & Schuler, H. (2011). Development and validation of the German work-related curiosity scale. *European Journal of Psychological Assessment*.
Muthén, L., & Muthén, B. (2016). Mplus. *The comprehensive modelling program for applied researchers: user's guide, 5*.
Niehaves, B., Köffer, S., & Ortbach, K. (2012). *IT consumerization–a theory and practice review*. Paper presented at the Eighteenth Americas conference on information systems.
O'Neill, T. A., & Hastings, S. E. (2011). Explaining workplace deviance behavior with more than just the "Big Five". *Personality and Individual Differences, 50*(2), 268-273.

Okolo, D. (2018). An exploration of the relationship between technostress, employee engagement and job design from the Nigerian banking employee's perspective. *Management Dynamics in the Knowledge Economy, 6*(4), 511-531.
Oppe, S. (1988). The concept of risk: A decision theoretic approach. *Ergonomics, 31*(4), 435-440.
Osborne, T. K. (2019). *Macro-level strain theory: examining the roles of strain, negative affect, emotion regulation, social support, and collective efficacy on community violence exposure and behavioral outcomes.* (MASTER OF ARTS), California State University,
Patel, J., Ryoo, S., & Kettinger, W. (2012). *Theorizing the dual role of information technology in technostress research*. Paper presented at the American Conference of Information Systems
Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, 105-136.
Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A Principal-Agent perspective. *MIS Quarterly, 31*(1), 105-136.
Penney, L. M., & Spector, P. E. (2005). Job stress, incivility, and counterproductive work behavior (CWB): The moderating role of negative affectivity. *Journal of Organizational Behavior, 26*(7), 777-796.
Pennington, R. R., Kelton, A. S., & DeVries, D. D. (2006). The effects of qualitative overload on technology acceptance. *Journal of Information Systems, 20*(2), 25-36.
Pham, H.-C., El-Den, J., & Richardson, J. (2016). Stress-based security compliance model–an exploratory study. *Information & Computer Security*.
Pirkkalainen, H., Salo, M., Makkonen, M., & Tarafdar, M. (2017). *Coping with technostress: When emotional responses fail.* Paper presented at the The 38th international conference on information systems.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879.
Pond, D. J., & Leifheit, K. R. (2003). End of an error. *Security Management, 47*(5), 113-113.
Porcelli, A. J., & Delgado, M. R. (2009). Acute stress modulates risk taking in financial decision making. *Psychological Science, 20*(3), 278-283.
Porter, L. W., Crampon, W. J., & Smith, F. J. (1976). Organizational commitment and managerial turnover: A longitudinal study. *Organizational Behavior & Human Performance*

15(1), 87-98.
Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551-567.
PWC. (2018). The Global State of Information security, Survey 2018. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
Ragu-Nathan, T., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research, 19*(4), 417-433.
Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139.
Reber, A. S. (1989). Implicit learning and tacit knowledge. *Journal of Experimental Psychology: General, 118*(3), 219.
Reio Jr, T. G., & Wiswell, A. (2000). Field investigation of the relationship among adult curiosity, workplace learning, and job performance. *Human Resource Development Quarterly, 11*(1), 5-30.
Renaud, K., & Privacy. (2011). Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security & Privacy, 10*(3), 57-63.
Reyna, V. F., & Farley, F. (2006). Risk and rationality in adolescent decision making: Implications for theory, practice, and public policy. *Psychological Science in the Public Interest, 7*(1), 1-44.
Richard, R. (2010). CSI Computer Crime and Security Survey. In *Computer Security Institute*.
Richardson, H. A., Yang, J., Vandenberg, R. J., DeJoy, D. M., & Wilson, M. G. (2008). Perceived organizational support's role in stressor-strain relationships. *Journal of Managerial Psychology, 23*(7).
Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Sarabadani, J., Carter, M., & Compeau, D. (2018). *10 Years of Research on Technostress Creators and Inhibitors: Synthesis and Critique*. Paper presented at the Twenty-fourth Americas Conference on Information Systems.
Sarabadani, J., Compeau, D., & Carter, M. (2020). *An Investigation of IT Users' Emotional Responses to Technostress Creators.* Paper presented at the Proceedings of the 53rd Hawaii International Conference on System Sciences.
Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112-133.
Sauner-Leroy, J. B. (2004). Managers and productive investment decisions: the impact of uncertainty and risk aversion. *Journal of Small Business Management, 42*(1), 1-18.
Sellberg, C., & Susi, T. (2014). Technostress in the office: a distributed cognition perspective on human–technology interaction. *Cognition, Technology & Work, 16*(2), 187-201.
Shaw, E. D., Post, J. M., & Ruby, K. G. (1999). Inside the Mind of the Insider. *Security Management, 43*(12), 34-42.
Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). *Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). *Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish.* Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security.
Singh, J. V. (1986). Performance, slack, and risk taking in organizational decision making. *Academy of Management Journal, 29*(3), 562-585.
Singh, T., Johnston, A., & Thatcher, J. (2019). *How Much is Too Much: Employee Monitoring, Surveillance, and Strain*. Paper presented at the Fortieth International Conference on Information Systems.
Siponen, M. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(1), 19.
Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.
Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.
Siponen, M. T., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.
Sloman, S. A. (1996). The empirical case for two systems of reasoning. *Psychological Bulletin, 119*(1), 3.
Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis, 24*(2), 311-322.
Sluss, D. M., Van Dick, R., & Thompson, B. S. (2011). Role theory in organizations: A relational perspective. In *Handbook of Industrial/Organizational psychology, Vol 1: Building and Developing the Organization.* (pp. 505-534): American Psychological Association.
Šotić, A., Mitrović, V., & Rajić, R. (2014). Risk perception during construction works execution. *Online JAKM, 2*(3), 44-55.
Stanton, J., Mastrangelo, P., Stam, K., & Jolton, J. (2004). Behavioral information security: Two end user survey studies of motivation and security practices. *Americas Conference of Information Systems*, 175.
Stich, J.-F., Tarafdar, M., Stacey, P., & Cooper, C. L. (2019). E-mail load, workload stress and desired e-mail load: a cybernetic approach. *Information Technology & People, 32*(2).
Strack, F., & Deutsch, R. (2004). Reflective and impulsive determinants of social behavior. *Personalitysocial Psychology Review, 8*(3), 220-247.
Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.
Strauss, A., & Corbin, J. (1990). *Basics of qualitative research*: Sage publications.
Tams, S., Hill, K., de Guinea, A. O., Thatcher, J., & Grover, V. (2014). NeuroIS-alternative or complement to existing methods? Illustrating the holistic effects of neuroscience and self-reported data in the context of technostress research. *Journal of the Association for Information Systems, 15*(10).
Tams, S., Thatcher, J. B., & Grover, V. (2018). Concentration, competence, confidence, and capture: An experimental study of age, interruption-based technostress, and task performance. *Journal of the Association for Information Systems, 19*(9), 2.

Tarafdar, M., Pullins, E. B., & Ragu-Nathan, T. (2015). Technostress: negative effect on performance and possible mitigations. *Information Systems Journal, 25*(2), 103-132.
Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan. (2007a). The impact of technostress on role stress and productivity. *Journal of management information systems, 24*(1), 301-328.
Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan. (2007b). The impact of technostress on role stress and productivity. *Journal of Management Information Systems, 24*(1), 301-328.
Tarafdar, M., Tu, Q., & Ragu-Nathan, T. (2010). Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems, 27*(3), 303-334.
Taylor, R. (2006). *Management perception of unintentional information security risks*. Paper presented at the International Conference on Information Systems
Teh, P.-L., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees?: Insights from neutralization and social exchange theory. *Journal of Global Information Management, 23*(1), 44-64.
Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: toward a conceptual model of utilization. *MIS Qquarterly*, 125-143.
Tippins, M. J., & Sohi, R. S. (2003). IT competency and firm performance: is organizational learning a missing link? *Strategic Management Journal, 24*(8), 745-761.
Tom, S. M., Fox, C. R., Trepel, C., & Poldrack, R. A. (2007). The neural basis of loss aversion in decision-making under risk. *Science, 315*(5811), 515-518.
Trevino, L. K. (1992). Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly, 2*(2), 121-136.
Trimpop, R. M. (1994). *The psychology of risk taking behavior* (Vol. 107): Elsevier.
Tu, Q., Wang, K., & Shu, Q. (2005). Computer-related technostress in China. *Communications of the ACM, 48*(4), 77-81.
Turel, O., & Gaudioso, F. (2018). Techno-stressors, distress and strain: the roles of leadership and competitive climates. *Cognition, Technology & Work, 20*(2), 309-324.
Turel, O., & Qahri-Saremi, H. (2016). Problematic use of social networking sites: antecedents and consequence from a dual-system theory perspective. *Journal of Management Information Systems, 33*(4), 1087-1116.
Ullman, J. B., & Bentler, P. M. (2003). Structural equation modeling. *Handbook of Psychology*, 607-634.
Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior, 78*, 283-297.
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198.
Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. *Annual Review of Sociology, 25*(1), 271-305.
Vigoda-Gadot, E. (2007). Redrawing the boundaries of OCB? An empirical examination of compulsory extra-role behavior in the workplace. *Journal of Business Economics & Psychology, 21*(3), 377-405.
Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586.
Wachira, P., & Keengwe, J. (2011). Technology integration barriers: Urban school mathematics teachers perspectives. *Journal of Science Education & Technology, 20*(1), 17-25.
Wall, T. D., Jackson, P. R., Mullarkey, S., & Parker, S. K. (1996). The demands—control model of job strain: A more specific test. *Journal of Occupational & Organizational Psychology, 69*(2), 153-166.
Wang, K., & Shu, Q. (2008). *The moderating impact of perceived organizational support on the relationship between technostress and role stress.* Paper presented at the 2008 19th International Workshop on Database and Expert Systems Applications.
Wang, K., Shu, Q., & Tu, Q. (2008). Technostress under different organizational environments: An empirical investigation. *Computers in Human Behavior, 24*(6), 3002-3013.
Wang, X., Tan, S. C., & Li, L. (2020). Technostress in university students' technology-enhanced learning: An investigation from multidimensional person-environment misfit. *Computers in Human Behavior, 105*, 106208.
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.

Warkentin, M., & Mutchler, L. (2014). Research in Behavioral Information Security Management. *Information Systems and Information Technology, 2*.
Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105.
Wehner, L. E., & Thies, C. G. (2014). Role theory, narratives, and interpretation: The domestic contestation of roles. *International Studies Review, 16*(3), 411-436.
Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015). Will the "Phisher-Men" Reel You In?: Assessing individual differences in a phishing detection task. *International Journal of Cyber Behavior, Psychology and Learning, 5*(4), 1-17.
Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.
Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.
Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science & Technology in Society, 58*(2), 212-222.
Wright, R. T., Campbell, D. E., Thatcher, J. B., & Roberts, N. (2012). Operationalizing multidimensional constructs in structural equation modeling: Recommendations for IS research. *Communications of the Association for Information Systems, 30*(1), 23.
Xu, Z., & Guo, K. (2019). It ain't my business: a coping perspective on employee effortful security behavior. *Journal of Enterprise Information Management, 32*(5).
Yan, Z., Guo, X., Lee, M. K., & Vogel, D. R. (2013). A conceptual model of technology features and technostress in telemedicine communication. *Information Technology & People, 26*(3).
Yates, J. F., & Stone, E. R. (1992). *The risk construct*: John Wiley & Sons.
Yu, L., Shi, C., & Cao, X. (2019). *Understanding the Effect of Social Media Overload on Academic Performance: A Stressor-Strain-Outcome Perspective.* Paper presented at the Proceedings of the 52nd Hawaii International Conference on System Sciences.
Yuan, F., & Woodman, R. W. (2010). Innovative behavior in the workplace: The role of performance and image outcome expectations. *Academy of Management Journal, 53*(2), 323-342.
Zaloom, C. J. (2004). The productive life of risk. *Cultural Anthropology, 19*(3), 365-391.
Zhang, S., Zhao, L., Lu, Y., & Yang, J. (2016). Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social network services. *Information & Management, 53*(7), 904-914.
Zuckerman, M. (1979). *Sensation seeking*: Wiley Online Library.
Zuckerman, M., & Kuhlman, D. M. (2000). Personality and risk-taking: common bisocial factors. *Journal of Personality, 68*(6), 999-1029.

APPENDICES

Table 2. A Measurement items and scales	
Techno-overload	I am forced by different types of technologies* to work much faster. I am forced by different types of technologies to do more work than I can handle. I am forced by different types of technologies to work with very tight time schedules. I am forced to change my work habits to adopt to new technologies. I have a higher workload because of increased technology complexity.
Techno-Invasion	I spend less time with my family due to using different types of technologies. I have to be in touch with my work even during my vacation due to using different types of technologies I have to sacrifice my vacation and weekend time to keep current on new technologies. I feel my personal life is being invaded by using different types of technologies.
Techno-Complexity	I don't know enough about new technologies to handle my job satisfactorily. I don't need to spend time to understand and use new technologies. ** I don't find enough time to study and upgrade my technology skills. I find my colleagues know more about technology than I do. I often find it too complex for me to understand and use new technologies.
Techno-Insecurity	I feel constant threat to my job security due to new technologies. I have to constantly update my skills to avoid being replaced. ** I am threatened by coworkers with newer technology skills. I don't share my knowledge with my coworkers for fear of being replaced. I feel there is less sharing knowledge among coworkers for fear of being replaced.
Techno-Uncertainty	TU1. There are always new developments in technologies we use in our organization. TU2. There are constant changes in computer software/hardware in our organization. TU3. There are frequent upgrades in computer systems and applications in our organization.
Techno-Unreliability	Due to dependency of my work activities to technology, I cannot do my primary work activities when there is a breakdown in systems. Due to dependency of my work activities to technology, I cannot do my primary work activities when computer speed or response time is slow (e.g., like hitting a button and there is a delay until it loads). I cannot do my primary work activities due to temporary unavailability of certain online services. I cannot do my primary work activities due to instability of internet connection.
Strain	I feel drained from activities require me to use technologies. I feel tired from my technology-related activities. Working all day with different types of technologies is a strain for me. I feel burned out from my technology-related activities.

Intention to violate ISP	How likely is that you would have done the same as Adam in that situation? (very unlikely/very likely). I could see myself sharing the password as Adam did. (Strongly disagree/Strongly agree)
Scenario Realism	How realistic do you think the scenario is? (Highly Unrealistic-Highly realistic)
* The term technology refers to any types of day-to-day computer-based applications or IoT devices you use, such as automatic scheduling, office automation systems, smart phones, smart watches, application development tools, email, smart mailbox, facial recognition system, voice to text devices, etc.). ****** Removed items due to low loading factor (<0.60)	

Table 2.B Scenarios	
Password-Sharing	Adam is an employee in your organization. One day while Adam is out of the office, one of his coworkers needs a file on Adams' computer. The coworker performs similar job functions to Adam's. The coworker calls Adams and asks for his account information. Although Adam knows your organization has a policy that password must not be shared, he shares his password with the coworker.
Password Write-Down	John is an employee in your organization. The organization recently installed a computer system for managing employee personal information (e.g., employee emergency contacts, retirement benefits, salary information). Each employee has been given a user name and password for the system. John is aware of the company policy stating users are required to keep their passwords to themselves and not let other people know or use them. However, finding it difficult to remember his password, John wrote it down on a sticky note and attached it to the computer he usually uses.
Failure to Logoff	Jim is an employee in your organization. As part of his job, Jim has been given authorised access to the company's payroll system. One day at work, Jim logs into the payroll system to gather information for a weekly report that he prepares for management. After some time, Jim needs a restroom break. He is aware of the company's policy that requires users to logoff their computers when not in use. However, Jim hates the inconvenience of logging out and logging back in again, so he does not log off his computer when he leaves his desk to visit the restroom.
USB Copy	Justin is an employee in your organization and is currently working on a report that requires the analysis of sensitive company data. He is extremely busy and wants to continue working on the report later that evening at home. Caleb is aware of your company's policy that prohibits users from copying company data to portable media, such as USB drives, to avoid security problems. However, Caleb copies several company files to his personal, unencrypted USB drive so he can work on the report at home.
Data Leakage	Alex is an employee in the human resources department at your organization and thus has been authorised to view the salary information of all employees as part of his job functions. Recently, one of Alex's friends (who does not work for your organization) contacted Alex and asked for the salary information of all managers in your organization. The friend informed Alex that he was applying for a management position in your organization and wanted to use the information to determine what salary to ask for in case he is offered the position. Although Alex believes providing the salary information is a violation of company policy, he looks it up and gives it to the friend.

Click on Links	Nathan is an employee in your organization and receives many e-mails every day containing links that take him to fill out some forms. One day he receives an email from an unknown sender. Even though it is against your organizations' policy to click on links without verifying the source of the email, he clicks on the link assuming the email is sent from reliable source.

Table 4. A. Measurement items and scales

Latent Variable	Item	Scale (5-Likert)	Mean	SD
Curiosity (Cur)	Cur1. I am interested in how my contribution impacts the company.	Strongly disagree-Strongly agree	3.88	0.93
	Cur2. I enjoy developing new strategies.		3.92	0.99
	Cur3. Regarding practical problems, I'm also interested in the underlying causes.		4.07	0.86
	Cur4. When confronted with complex problems, I like to look for new solutions.		4.02	0.88
	Cur5. I enjoy pondering and thinking.		4.06	0.96
	Cur6. I am eager to learn new things.		4.23	0.86
	Cur7. I keep thinking about a problem until I solve it.		4.09	0.90
	Cur8. I challenge already existing concepts critically.		3.79	0.97
	Cur9. I carry on seeking information until I am able to understand complex issues.		4.08	0.91
	Cur 10. I try to improve work processes by making innovative suggestions.		3.96	1.0
Impulsivity (IMP)	Imp1. I plan tasks carefully. (Non-planning) *	Rarely/Never-Always * All are reverse coded items. +Items for motor dimension were not included in the model.	2.05	0.93
	Imp2. I plan trips well ahead of time. (Non-planning) *		1.97	0.98
	Imp3. I plan for job security. (Non-planning) *		2.27	1.14
	Imp4. I am future oriented. (Non-planning) *		2.26	1.01
	Imp5. I am self-controlled. (Attention)*		2.07	0.91
	Imp6. I concentrate easily. (Attention)*		2.08	0.89
	Imp7. I am a careful thinker. (Attention)*		1.92	0.90
	Imp8. I am a steady thinker. (Attention)*		1.91	0.86
	Imp9. I don't pay attention. (Attention)+		-	-
	Imp10. I say things without thinking. (Motor) +		-	-
	Imp11. I act on impulse. (Motor) +		-	-
	Imp12. I do things without thinking (Motor) +		-	-
	Imp13. I act in the spur of the moments. (Motor)+		-	-

Risk-Taking Behavior (RTB)	Rtb1. I will take risks at work in order to get the best results, even though my efforts might fail. Rtb2. I will take a risk and try something new if I have an idea that might improve my work, regardless of how I might be evaluated. Rtb3. When I think of a good way to improve the way I accomplish my work, I will risk potential failure to try it out. Rtb4. I am willing to risk potential failure when I have a good idea that could help me become more successful. Rtb5. I don't think twice about taking risks in my job if I think they will make me more productive, regardless of whether or not my efforts will be successful. Rtb6. Even if failure is a possibility, I will take risks on the job if I think they will help me reach my goals. Rtb7. When I think of a way to increase the quality of my work, I will take a risk and pursue the idea even though it might not pan out. Rtb8. In an effort to improve my performance, I am willing to take risks with my work, even if they may not prove successful.	Strongly disagree-Strongly agree	2.97 3.04 3.14 3.20 2.70 3.03 3.17 3.13	1.14 1.19 1.19 1.14 1.22 1.16 1.08 1.20
Information Security Awareness (ISA)	Isa1. Overall, I am aware of the potential information security threats and their negative consequences (e.g., personal information exposure). Isa2. I have sufficient knowledge about the cost of potential security problems. Isa3. In general, I understand the concerns regarding information security and the risks they pose. Isa4. I know and understand the rules and regulations prescribed by the information security policy of my organization. Isa5. I know my responsibilities as prescribed in the information security policy to enhance the IS security of my organization.	Strongly disagree-Strongly agree	4.18 4.14 4.23 4.23 4.18	0.78 0.90 0.82 0.86 0.89
Perceived Work-overload (PWO)	Pwo1. In my workplace, I feel that the number of requests, problems, or complaints I deal with is more than expected. Pwo2. When I am at work, I feel that the amount of work I do interferes with how well it is done.	Strongly disagree-Strongly agree *Removed item because of low loading (<0.5).	2.78 2.68 3.12	1.13 1.21 1.17

	Pwo3. In my workplace, I feel busy or rushed. * Pwo4. In my workplace, I feel pressured.			
Non-malicious Information Security Misbehavior (NISM)	Nism1. I share passwords with friends and colleagues. Nism 2. I use or create simple passwords (e.g., family name and date of birth). Nism 3. I use the same password for multiple websites. Nism 4. I use online storage systems to exchange and keep personal or sensitive information (e.g., Dropbox, Google Drive). Nism 5. I submit information to websites without checking their security information/certification. Nism 6. I use free public Wi-Fi. Nism 7. I check whether the programs and anti-virus software that I use are up-to-date.* Nism 8. I download applications from an unknown source. Nism 9. I disable the antivirus on my work computer in order to download information from websites. Nism 10. I download digital media without verifying the license of the sources. Nism 11. I click on links that I receive without checking the source of the email they came in. Nism 12. I send personal information to others over the Internet. Nism 13. I open links contained in an email from a trusted friend or work colleague without verifying where it leads. Nism 14. I download data and material from websites on my work computer without checking its authenticity.	Rarely/Never-Always *Removed item because of low loading (<0.5).	1.34 1.69 2.18 2.09 1.71 2.09 - 1.45 1.38 1.80 1.39 1.78 1.73 1.44	0.75 1.13 1.21 1.27 1.04 1.01 - 0.88 0.89 1.19 0.91 0.90 1.07 0.93

VITA

Forough Nasirpouri Shadbad

Candidate for the Degree of

Doctor of Philosophy

Dissertation: UNDERSTANDING EMPLOYEE NON-MALICIOUS INTENTIONAL AND UNINTENTIONAL INFORMATION SECURITY MISBEHAVIORS

Major Field: Business Administration

Biographical:

Education:

Completed the requirements for the Doctor of Philosophy in Business Administration at Oklahoma State University, Stillwater, Oklahoma in May, 2021.

Completed the requirements for the Master of Science in Physics at University of Tabriz, Iran in 2011.

Completed the requirements for the Bachelor of Science in Physics at University of Tabriz, Iran, 2008.

Experience:

Graduate Research/Teaching Associate at Oklahoma State University, 2017-2021

Professional Memberships:

Association of Information Systems (AIS), Institute for Operations Research and the Management Sciences (INFORMS)