

Louisiana Tech University

Louisiana Tech Digital Commons

Doctoral Dissertations

Graduate School

Winter 2-2022

Security-Related Technostress Trifecta on Employees' Security Counterproductive Behaviors

Bao Duong

Follow this and additional works at: <https://digitalcommons.latech.edu/dissertations>

**SECURITY-RELATED TECHNOSTRESS TRIFECTA ON
EMPLOYEES' SECURITY COUNTERPRODUCTIVE
BEHAVIORS**

by

Bao Duong, B.A., M.B.A., B.B.A.

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Business Administration

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

February 2022

LOUISIANA TECH UNIVERSITY

GRADUATE SCHOOL

December 7, 2021

Date of dissertation defense

We hereby recommend that the dissertation prepared by

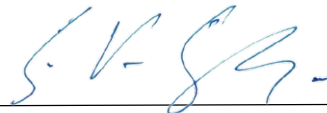
Bao Duong, M.B.A., B.B.A.

entitled **Security-Related Technostress Trifecta on Employees' Security**


Counterproductive Behaviors

be accepted in partial fulfillment of the requirements for the degree of

Doctor of Business Administration, Computer Information Systems Concentration



Craig Van Slyke, Supervisor of Dissertation Research




Selwyn Ellis,
Head of Computer Information Systems

Members of the Doctoral Committee:


Jaeung Lee
Selwyn Ellis

Approved:



Christopher Martin
Dean of Business

Approved:



Ramu Ramachandran
Dean of the Graduate School

ABSTRACT

Information security technology has become more important in preventing and protecting organizational digital assets, and employees are often considered the last line of defense. However, employees at all levels have to face and deal with the complexity, overload, and uncertainty of information security technology in their jobs every day. Although information security technology could benefit the organization and individual employees as it is critical to building and strengthening protection mechanisms for organizational digital assets and employees' data, it could also negatively affect employees' emotions and work accomplishments.

This study examines the two effects of psychological techno-stress responses (security-techno distress and security-techno eustress) are caused by information security techno-stressors, which eventually influence security counterproductive behavior. In addition, a quantitative investigation with a cross-sectional survey design to collect data that measured items reflect the constructs discussed in the above section will be considered to evaluate the hindrance and challenge security techno-stressors that predict emotional security-techno distress and security techno-eustress response that may lead to the security counterproductive behavior. The findings suggested that security job demands are positively associated with security-techno distress and security-techno eustress, suggesting that if there is no demand, there is no challenge or motivation for employees to improve their security best practice. Meanwhile, security job resources

This study has theoretical and practical implications for information security scholars and practitioners. It had negative significant impacts on security-techno distress and positive significant effects on eustress, which suggested that these factors encourage employees to prepare well for challenges interacting with information security technology. Overall, this research increases the understanding of information security technostress and the essential role of distress and eustress on security counterproductive behavior.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Dissertation. It was understood that “proper request” consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Dissertation. Further, any portions of the Dissertation used in books, papers, and other works must be appropriately referenced to this Dissertation.

Finally, the author of this Dissertation reserves the right to publish freely, in the literature, at any time, any or all portions of this Dissertation.

Author _____

Date _____

TABLE OF CONTENTS

ABSTRACT.....	iii
APPROVAL FOR SCHOLARLY DISSEMINATION	v
LIST OF TABLES	viii
LIST OF FIGURES	ix
ACKNOWLEDGEMENTS	x
CHAPTER 1 INTRODUCTION	1
Purpose of Study.....	4
Significance of Study.....	8
CHAPTER 2 LITERATURE REVIEW	10
Theoretical Background.....	12
Security-Related Hindrance Techno-Stressors	15
Security-Related Challenge Techno-Stressors.....	19
Distress and Eustress.....	24
Security Counterproductive Behavior.....	28
Research Model and Hypotheses	31
CHAPTER 3 RESEARCH METHODOLOGY	39
General Approach.....	39
Measures	40

Pilot Test	46
Pilot Test Reliability Analysis	46
Power Analysis	52
Actual Data Collection Procedures	52
CHAPTER 4 DATA ANALYSIS	55
Descriptive Statistics.....	56
Measurement Model	56
Common Method Variance.....	63
Structural Model	64
CHAPTER 5 DISCUSSION AND CONCLUSIONS	69
Theoretical Contributions	73
Practical Contributions.....	74
Limitations and Future Research	77
REFERENCES	80
APPENDIX A HUMAN USE APPROVAL LETTER	92
APPENDIX B SCREENING QUESTIONS	94
APPENDIX C POWER ANALYSIS	96
APPENDIX D WORKER REQUIREMENTS.....	98

LIST OF TABLES

Table 2.1	<i>Definitions and Constructs Used in Study</i>	30
Table 3.1	<i>Constructs, Adapted Items, and Sources</i>	42
Table 3.2	<i>Cronbach's Alpha Values of Security Techno-Uncertainty, Technical Support, and Eustress</i>	47
Table 3.3	<i>Measurement of Outer Loadings of the Eustress</i>	48
Table 4.1	<i>Demographics</i>	56
Table 4.2	<i>Construct Reliability and Validity</i>	58
Table 4.3	<i>Correlations Table</i>	59
Table 4.4	<i>Cross Loading</i>	61
Table 4.5	<i>Results</i>	65
Table 4.6	<i>Total Effects of Antecedent Variables on Security Counterproductive Behaviors</i>	68

LIST OF FIGURES

Figure 2.1: <i>Conceptual Framework</i>	38
Figure 4.1: <i>Model Result</i>	67

ACKNOWLEDGEMENTS

I want to express my gratitude and praise God for several individuals that deserve specific mention for their role in providing unconditional support to my progress in the doctoral program at Louisiana Tech University.

First, two of the greatest blessings God has given me are my father, Thang Q. Duong, and my mom, Mai T.H. Tran, whose sacrifice, hard work, and strong belief toward their son's success have built a foundation for me to be where I am today. There is no word that I can express my gratitude toward my parents.

Second, I must mention my wife, Tram T.N. Le, who has been with me through sunny and rainy days. None of my progress in the doctoral program would have been possible without her. She is my support system, providing unconditional love and motivating me to move forward even when things go unexpectedly.

Third, to my dissertation chair, Dr. Craig Van Slyke, for his unconditional support, inspiration, and outstanding leadership, always encouraging me to go the extra mile in research. His invaluable guidance of my dissertation and research seminars taught me precious lessons that I value every comment concerning what is worthwhile in my research streams in IS discipline. Without his wisdom and motivation, I could not have accomplished all I did. Fourth, to my dissertation committee member, Dr. Jae-ung Lee, for his mentorship and guidance during my very first year in the doctoral program, and Dr. Selwyn T. Ellis for his effective leadership, great sense of humor, and caring toward

doctoral students' success. His administration is one of the key factors that keep the CIS Department growing and moving forward. Also, thanks to Dr. Tom Stafford for his support and my progress and wisdom in research that strengthened my qualitative research skills.

Last but not least, I would like to thank the professors who taught me during the doctoral program at Louisiana Tech. Dr. Hani Mesak, Dr. Bruce Alford, Dr. Ghislain NoNo Gueye, Dr. Marcia Dickerson, and Dr. Jeffrey Haynie. Their knowledge, wisdom, and effort have transformed my life and research capability. I am incredibly grateful to have these great people with me along the way from start to finish my dissertation.

CHAPTER 1

INTRODUCTION

The growing prevalence of high-profile cybersecurity attacks associated with potential data breaches impact organizations and consumers since companies and consumers rely on online networks to conduct business transactions and communication (Spitzer, 2020). At the same time, the growing risk of potential security breaches pushes organizations and consumers to increase investment in information security technology to battle various security threats. According to a Gartner forecast report, worldwide spending on information security by 2022 was expected to reach a total of \$133.8 billion (Moore, 2020). In the U.S., revenue for security-related software and services is estimated at \$20.8 billion over the five years to 2025 and is forecasted to sustain an annual growth rate of 4.1 % (Spitzer, 2020). Firms invested heavily in information security technology to mitigate or prevent security incidents and threats by strengthening new security management and critical information control. Nevertheless, a cyber-stress report's findings showed that 81 percent of Americans still admit that cybersecurity issues (e.g., virus, ransomware attack, social engineering attacks) have drawn increasing attention and discussion in organizations and consumers (Kaspersky, 2019). The ongoing anxiety of ever-growing cyber threat offense and organizations' defense aims to protect data stored on Information Technology (IT) devices (e.g., computers, mobile devices) and cloud servers devices and data from unknown threats underlies our long-term

cyber-stress issues as the advancements in information security technology provide us with incredible opportunities and quickly cause people to feel lost and stressed. Stress is defined as the ongoing interaction between an individual and the surrounding environment; an individual perceives it as taxing that exceed available resources or affects the individual's well-being and behavior (Cooper et al., 2001; Tarafdar et al., 2017). More importantly, stress costs U.S.-based employers an estimated \$300 billion each year, according to the American Institute of Stress (AIS, 2019). The individual consequences of workplace stress are physical and psychological issues that often affect employees' work performance and lead to employee turnover, disengagement, and absenteeism.

The information security (InfoSec) literature suggests that human elements are considered the last line of defense and the weakest link against cyberattacks (Kirsch & Boss, 2007; Bulgurcu et al., 2010; Posey et al., 2014; Zimmermann & Renaud, 2019). Although information security technology has been heavily invested and users adopt new technological devices to support compliant information security systems procedures (e.g., email encryption, virtual private networks, identity management, multiple-factor authentication), the number of systems that employees need to use increases with specific information systems security requirements, and the mandatory technical prompts (system-specific criteria for changing password) or adjustable (e.g., computer or system locks itself automatically after a certain period), people who are affected by the new information systems security are largely ignored (Zimmermann & Renaud, 2019).

Moreover, findings suggest that conflicts between complying with cybersecurity policies and prioritizing work-related tasks are important drivers of non-compliance.

(Kirlappos et al., 2013; Hwang et al., 2016). The current cyber threat landscape requires organizations and employees to improve cybersecurity approaches and evaluate information security technology' effectiveness for avoiding technology overload; thus, it is important to help employees tackle information security negative stress response while at the same time strengthening understanding of benefits from information security technology and process have in place (Zimmermann & Renaud, 2019).

D'Arcy et al. (2014) derived security-related stress (SRS) from the technostress literature. They found that SRS has a significant positive relationship with moral disengagement to predict information security policy (ISP) violating behavior. However, compounding this program, information security technology stress often bleeds over into employees' offices with the potential to security and privacy breaches penetrated or circumvents information security controls embedded into individual information technology work devices (Mamonov & Benbunan-Fich, 2018; Thompson et al., 2017). Moreover, employees need to build up their information security knowledge to protect organizational digital assets since the current information security ongoing threat landscapes require constant updates on information security technology that require individual capabilities of self-motivated in adapting and learning new information security technology (Karjalainen et al., 2019).

A stressor is an event, demand, stimulus, or condition that an individual may experience in the workplace environment (Cooper et al., 2001; Cooper & Dewe, 2008). Little research has examined security-related techno stressors. Previous studies developed security technostress models on general information security stress perceptions (i.e., role stress related to information security) and linked them to security compliance intention

(Hwang & Cha, 2018; Hwang & Cha, 2021). Demands are characteristics associated with physiological and psychological costs within the workplace environment (Bakker & Demerouti, 2007; Bakker & Demerouti, 2017). Stressors often stimulate an individual's stress responses, which eventually influence psychological and behavioral outcomes (Simmons & Nelson, 2001; Hargrove et al., 2013; Califf et al., 2020). This study investigates the antecedents and outcomes of two distinct types of information security technostress sub-process: security-techno distress, which results in negative responses to stressors, and security techno-eustress, which results in positive responses to stressors. Building a holistic of security techno-stressors that influence both security-techno distress and security-techno eustress responses, the theoretical framework of Job Demands-Resources was incorporated with the technostress trifecta to identify and examine empirically challenge and hindrance security-related techno stressors. Their association with negative and positive psychological stress responses (security-techno distress and security-techno eustress) potentially predicts a negative behavioral outcome called security counterproductive behavior. Challenge techno-stressors are defined as characteristics of IS that are perceived to provide an opportunity to improve and strengthen individuals' skills, tasks, and work-life. On the other hand, hindrance techno-stressors are referred to as IS characteristics perceived as damaging, interrupting, and affecting individuals' work accomplishment and often associated with positive work-related outcomes (Cavanaugh et al., 2000; LePine et al., 2004; Podsakoff et al., 2007).

Purpose of Study

Previous studies have depicted a negative landscape of security-related technostress by positing that security-related techno stressors are harmful to employees'

work performance. Findings suggest negative consequences of security-related stress toward moral disengagement, neutralization, and decreasing organizational commitment and organizational security policy compliance (D'Arcy et al., 2014; D'Arcy & Lowry, 2019; D'Arcy & Teh, 2019). However, previous studies suggested a positive relationship between techno stressors and psychological and behavioral outcomes such as productivity and performance (Califf et al., 2020; Tarafdar et al., 2010; Tarafdar et al., 2011). Reports find that many organizational insiders feel responsible for taking precautions against security threats, yet relatively few employees feel confident in their ability to protect their firms (Dell, 2017). Recent studies have called for understanding various emotions when dealing with techno-stressors (Califf et al., 2020; Tarafdar et al., 2017).

Besides, not all stress is detrimental to employees' well-being. Stressors viewed as beneficial result in positive stress responses (eustress), while those perceived as detrimental may result in negative stress responses (distress). Eustress is a form of stress response to a stressor perceived as beneficial in learning and accomplishing work-related goals, whereas distress responses negatively affect well-being (Califf et al., 2020; Selye, 1974; Simmons & Nelson, 2007; Tarafdar et al., 2017). There are calls for theoretical development in the technostress domain by investigating the distress and eustress within more specific IS contexts (Ayyagari et al., 2011; Califf et al., 2020; Tarafdar et al., 2017). People assess stressors in the context of their environment. For example, individuals base their appraisal of stressors on the light of how a particular stressor benefits or harms the accomplishment of work tasks (Tarafdar et al., 2015; Califf et al., 2020). In this study, it is argued that information security technology could benefit the organization and individual employees as they are critical to building and strengthening protection

mechanisms for organizational digital assets and employees' data. These information security technologies got more interwoven with employees' work-related tasks and burden employees with extra security demands due to constantly evolving threat landscapes such as ransomware and phishing spillover from workplace to personal devices (Li et al., 2019; Wang et al., 2017).

Distress and eustress responses can result from the same stressor, representing distinct constructs rather than the opposite ends of the same continuum (Edwards & Cooper, 1988; Nelson & Cooper, 2007). Negative appraisals occur when an individual anticipates that a stressor represents a threat of future harm or losses. These appraisals result in distress. In contrast, a positive appraisal, which brings about eustress, occurs when a person anticipates that some benefit will come because of the stressor. Both eustress and distress can be brought on by the same stressor (Hargrove et al., 2015). For example, a promoted worker may simultaneously appraise the promotion (a stressor) as likely to bring benefits, such as increased prestige, and harm, such as increased strain, resulting in both eustress and distress. This study defines information security technology stress response as psychological stress due to bundles of information security technology employees interact with during their regular work routine. The stresses could include password managers, antivirus software and customized firewalls, a virtual private network (VPN), multifactor authentication technology, and cloud security.

Overall, SRS is considered a hindrance stressor, which arises when employees perceive information security requirements as obstacles to their main job-related tasks and show negative reactions (D'Arcy et al., 2014; D'Arcy et al., 2018; D'Arcy & Ted, 2019). Security-related stressors are often a negative aspect of organizational information

security compliance (D'Arcy et al., 2014; D'Arcy et al., 2018; D'Arcy & Teh, 2019; Lee et al., 2016). However, a broader reading of the organizational stress literature suggests that techno-stressors could have positive and negative psychological responses (techno distress and techno eustress) (Califf et al., 2020; Hargrove et al., 2013; Tarafdar et al., 2017). To design a more effective security program, understanding information security techno-stressors that provide opportunities to improve and enhance employees' skills and tasks is important. While some research efforts address deterring bad end-user behavior arising from security-related stress, little effort has been made to promote the good stress end users may have that may lead to information security-related technology behaviors. Besides, "human as solution" is proposed to improve the design of information security technology interfaces to enhance usability to align with human needs and limitations (Zimmermann & Renaud, 2019). This study attempts to incorporate and identify an empirically testable challenge and hindrance security techno-stressors, their association with the consequences of security-techno distress and security-techno eustress responses, namely positive and negative psychological stress responses to security techno-stressors, which affect the inappropriate security counterproductive behavior.

This study is intended to make both theoretical and practical contributions to the information security and technostress literature. Job Demands-Resources (JD-R) (Demerouti et al. 2001) and Technostress-trifecta theoretical framework (Tarafdar et al., 2017) would make a theoretical contribution to InfoSec and technostress literature that may broaden the knowledge of stress using the security-related techno stressors. This study's theoretical contribution results from integrating the JD-R framework with the information security technology context. To the best of our knowledge, this is the first

research attempt to examine the two distinct types of information security technostress sub-processes, namely, security security-techno distress, which results in negative responses to stressors security-techno eustress, which results in positive responses. Second, this study examines and explores the differential effects of information security demands and resources on counterproductive security behavior.

Therefore, this research aims to answer the following research questions:

1. What are the potential consequences of two distinct types of information security technostress sub-processes on the behavioral outcome, security counterproductive behavior?
2. Which information security-techno stressors influence security counterproductive behavior?

Significance of Study

Employees at all levels have to face and deal with the complexity, overload, and uncertainty of cybersecurity in their jobs every day. Employees might have to deal with various situations where the organization's information security compliance goal interferes with employees' goal of efficiently completing work tasks, bringing about stress and negatively affecting security compliance. Little attention has been given to how stressful demands affect employees' information security techno-stress responses (distress and eustress) and security counterproductive behavior. Cram et al. (2019) meta-analysis study suggested that research in security needs to be more specific in terms of policy compliance due to different factors (i.e., specific information security technology that may impact on employee's compliance to protect organizational digital assets) as previous studies have either studied the broad spectrum compliance with general security

policies (i.e., a broad, all-encompassing, generic security policy), while others focused on compliance with a specific type of security policy (i.e., antivirus software, internet use, data backups).

This study contributes to practice by providing practitioners with a better understanding of how employees may engage in security counterproductive behaviors. Also, given the increasing number of employees affected by security stress at work, this study's findings may help practitioners understand the consequences of security techno-distress and techno-eustress responses, which are negative and positive psychological responses to security techno stressors. Finally, the study's findings could advise organizations to consider and distinguish good security techno-stressors from bad ones that influence employees' security counterproductive behavior, foster employees' commitment, and design programs that track and help employees mitigate the negative stress response.

CHAPTER 2

LITERATURE REVIEW

In this chapter, drawing from the InfoSec literature, technostress, and JD-R in the management and psychology disciplines, the relationship among the study's constructs are analyzed by building upon existing work for supporting theorizing and methodology.

Technostress is defined as stress experienced by individuals due to information technology, which is caused by an inability to cope with new technologies properly (Brod, 1984). The workplace has been digitally transformed, and employees have become more reliant on IT to fulfill work-related tasks. Due to dependency on IT, employees often experience technostress, including overload, complexity, uncertainty, and insecurity associated with IT (Tarafdar et al., 2007). Person-technology fit was contextualized and posited that technology features may cause a person-technology gap by either needs-supplies or demands-abilities misfits (Ayyagari et al., 2011; Tarafdar et al., 2015). The literature on IS technostress is abundant with studies that attempt to explain technostress factors' influence on negative psychological responses to stressors and organizational outcomes, including strain, job satisfaction, organizational commitment, withdrawal (Ayyagari et al., 2011; Lee et al., 2016; Shih et al., 2013; Ragu-Nathan, 2008; Tarafdar et al., 2007; Tarafdar et al., 2010; Tarafdar et al., 2015; Tams et al., 2018). Technostress studies have focused on the negative stress response, while positive stress response has been under-studied (Califf et al., 2020).

Technostress was adapted to and extended in the context of information security; nevertheless, the effect of technostress on employee security-related behaviors has been understudied (D'Arcy et al., 2014; Hwang & Cha, 2018). The literature on behavioral information security seems to lack consideration of the impact of security technologies on employees' security behavior, especially security counterproductive behavior. Previous studies looked at both technostress and employee ISP violation (D'Arcy et al., 2014; Hwang & Cha, 2018). For example, users might refuse to comply with ISPs if they find security tasks stressful due to complexity or uncertainty. Nevertheless, the literature on behavioral information systems security seems to lack consideration of the impact of IT on employees' extra-role activities like ISP compliance.

In this study, the theoretical frameworks of JD-R and Technostress-trifecta were incorporated to explore and examine the relationship between techno-stressors and two distinct types of information security technostress sub-processes, namely, security security-techno distress, which results in negative responses to stressors, and security-techno eustress, which results in positive responses. Also, JD-R suggests that job demands and resources initiate and affect exhaustion and organizational and behavioral outcomes (Bakker et al., 2003; Schaufeli & Bakker, 2004). This study focuses on the behavioral outcome of security counterproductive behavior. It examines the relationship between two distinct types of information security technostress sub-processes (security-techno distress and security-techno eustress) and security counterproductive behavior.

Theoretical Background

The Job Demands-Resources (JD-R) theoretical framework was originally used to explain employee burnout; however, it is recently recognized as an appropriate framework for explaining various facets of job stress (Bakker & Demerouti, 2007). In this study, the JD-R with Techno-stress trifecta was integrated to develop a research model and hypotheses on the effects of security techno stressors in employees' security behaviors. The model adapted security techno-stressors as job demands. As such, job demands refer to psychological, social, or organizational factors connected with the job that require sustained psychological effort and thus are associated with psychological and physiological costs such as exhaustion and disengagement (Demerouti et al., 2006, Ahuja et al., 2007). According to JD-R, all job characteristics can be classified as either job demands or job resources that make the theoretical framework flexible and popular across diverse disciplines (Bakker & Demerouti, 2014). Job resources are physical, mental, social, or organizational job characteristics offered to employees to accomplish work-related tasks and promote growth in learning and practice (Demerouti et al., 2006; Demerouti & Bakker, 2011). Whereas job demands can evoke psychological or organizational aspects that hinder organizational outcomes, job resources instigate motivational processes that positively affect employees' job performance (Bakker & Demerouti, 2017). Researchers have successfully applied the model in the information security context to explore and examine organizational factors that influence employees' security compliance burnout and security compliance (Pham et al., 2016; Pham et al., 2019).

Previous studies focused on examining different aspects of security-related job stress mainly focused on compliance intention (D'Arcy et al., 2014; D'Arcy & Teh, 2019b; Hwang & Cha, 2018; Pham et al., 2019), yet largely ignore how security technology may have both negative and positive impacts on employees' psychological and behavioral outcomes. Recent studies have called for a better and broader understanding of the two-sided effects of technology impact on employee' organizational outcomes (Califf et al., 2020) and for shifting the dominant perspective from treating "human-as-error" to treating "human-as-solution" (Zimmermann & Renaud, 2019). Within the information security context, it may be that "appropriate amounts of stress can positively affect employees' work performance" (Tarafdar et al., 2017; Zimmermann & Renaud, 2019). However, most studies point out the adverse effects of overwhelming stress on employees (Hwang & Cha, 2018, page 290). It is largely neglected that protecting organizations by enhancing information security technology might have unexpected results; ever-changing and complex information security technology and procedures might leave people inside the organizations in a stressful situation dealing with overload, information complexity, and uncertainty.

The JD-R model is a stress model that was originally designed to explain the antecedents of burnout, where job demands and job resources were identified as the possibility to cause burnout (Demerouti et al., 2001). Essentially, JD-R proposes that work has two general factors that affect job stress: job demands and resources. Job demands are the physical, social, or organizational aspects of the job which require individuals to put physical and psychological effort to deal with them (Bakker et al., 2003; Demerouti et al., 2001; Schaufeli & Bakker, 2004). Examples of job demands

include role conflict, role ambiguity, job insecurity, time pressure (Armstrong et al., 2015; Schaufeli & Taris, 2014). In contrast, job resources are defined as physical, organizational, social, and psychological aspects of the job that are helpful with individual development and skills learning through work-related tasks accomplishment and mitigating job demands and their associated psychological cost (Demerouti et al., 2001). Previous studies include feedback, autonomy, social support, and job resources (Schaufeli & Taris, 2014; Schaufeli & Bakker, 2004). The JD-R theoretical framework allows this study to examine the stressful demands and the motivational resources aspect of security-related technology that employees often must get involved in an organization.

The term ‘technostress’ was originally used to describe organizational and psychological decrements that could be attributed to the sustained efforts required by employees to remain proficient in changing information and communication technology (ICT) domains (Ragu-Nathan et al., 2008; Tarafdar et al., 2007). However, more recently, the idea of technology-induced stress has been extended to users of information security technology (Hwang & Cha, 2018; Hwang & Cha, 2021). Therefore, the technostress trifecta proposed the holistic IS design principles for technostress that include both techno-eustress and techno-distress to enhance the positive stress responses and mitigate the negative effects of technostress through appropriate design based upon different information technology contexts.

This study integrated the JD-R with the technostress trifecta framework to explain both the security techno-stressors and the psychological positive and negative stress responses (distress and eustress) eustress, which is defined as a positive response to a stressor that is perceived as beneficial in achieving goals and improving well-being.

While distress as stress that creates a threat or hindrance may serve as the guiding point to see which security-related stress may be perceived as eustress and distress, it will eventually impact employees' security inappropriate counterproductive behavior.

Security-Related Hindrance Techno-Stressors

Factors that induce stress are called stressors, and technology-related stressors are known as technostress creators or techno stressors (Tarafdar et al., 2010; Ragu-Nathan et al., 2008). Techno stressors were used in different contexts to understand which aspects of information technology affect employees' psychological and behavioral outcomes (Ayyagari et al., 2011; Galluch et al. 2015; Ragu-Nathan, 2008; Shih et al., 2013; Tarafdar et al., 2007; Tarafdar et al., 2010; Tarafdar et al., 2015; Tams et al., 2018).

Security-related stress (SRS) describes the stressful demands imposed explicitly by security policy requirements (D'Arcy et al., 2014). SRS is a form of psychological stress caused by internal or external security-related demands appraised as taxing one's cognitive resources or abilities incurred by security policy and procedures (D'Arcy et al., 2014). Even though the term SRS was adopted and developed from technostress literature, it was not explicitly examined in the stress-induced state of information security technology. There are three factors used: SRS-Overload, SRS-Complexity, SRS-Uncertainty.

Security-related technostress creators are defined as the degree of overload, complexity, and uncertainty of information security technology that cause employees psychological stress (Hwang & Cha, 2018). The reasons are that security technology is often complex, and systems adopted as security measures to improve information security often add challenges and demands on the employees, which often hinder their tasks

fulfillment and affect information security practice. Concerns arise that security technology stimulates employees' negative stress responses, as examined in this study. Adding new information security technology may hinder employees from achieving their work-related goals (Hwang & Cha, 2018). They may perceive security as not their primary work goal, creating additional work or conflict with their task fulfillment. The unique difference between SRS and the security technostress is that SRS contains security policies and procedures while the security technology aspect was largely ignored. Arguably, it is crucial to identify technology characteristics that are important to the context of information security technology. The reason is that the frequent interaction between users and security technology is critical to the design of information security management that improves value alignment for all parties involved as people, technology, and process are all needed to adequately secure a system (Merkow & Breihaupt, 2014).

Therefore, it is essential to identify technology characteristics that are important to the context of information security technology and stress. Moreover, there is a call to examine further characteristics of technostress related to information security technology to understand their unique impact on employees (Hwang & Cha, 2018). In this study, security technostress creators' rationale was adapted as security-related hindrance technostressors. The following paragraphs explain the unique difference between three factors from security-related stress and security technostress.

SRS-overload is defined as situations where security requirements increase employees' workload, leading to added time pressure to complete job duties (D'Arcy et al., 2014). Examples of SRS-overload were given in situations where security policy and

procedures' requirements increase the workload for employees and create added time pressure to meet these security requirements. That wastes employees' time on valuable tasks as they must follow the policy and procedures while trying to accomplish their work-related tasks. For example, there are many government regulations and industry standards (e.g., Payment Card Industry Data Security Standard (PCI-DSS) and Sarbanes-Oxley Act Section 404 (SOX 404)) that require organizations to follow certain procedures strictly.

On the other hand, security techno-overload refers to increased workload due to required information security technology. For example, in order to protect documents, employees may be required to get permission from the IT department before they exchange documents with clients and external partners or wait for IT staff to install software or download needed materials or automated employee' work task disruption due to virus scan or patch update. The increased use of information technology such as multifactor authentication (MFA) or a secure file transfer appliance requires employees to significantly change their work practices and habits, thereby contributing to greater stress.

SRS-Complexity refers to situations where security requirements are viewed as problematic and force employees to spend more time and effort learning and understanding security policies and procedures within the organization (D'Arcy et al., 2014). Examples are complex contingencies or technical jargon within security policies that inhibit employees' job task resources and increase stress.

More specifically focused on security technology, security techno-complexity is another factor related to circumstances in which the level of security technology required

is complex, such as frequent change or sudden updates. Security techno-complexity refers to the degree of complexity of information security technology, an inherent quality of information security technology that makes employees feel confused and incompetent. The information security technology requirement is modified to suit such a change; for instance, they find it difficult to determine when encryption is required. Organizations often require employees to spend extra time and effort to understand complex security technology terms, concepts and follow standardized processes and methodologies regardless of their work duties.

SRS-uncertainty refers to events that force organizations to continuously add and update security policies requirements (D'Arcy et al., 2014). Examples of internal and government or industry regulations law require new encryption rules for transmitting data and authentication procedures for accessing corporate systems. Also, the organization's updated security policy requires employees to adjust to new requirements, which are stress-inducing.

More specially focused on security technology, the security techno-uncertainty refers to the degree of change in employees' work due to constant upgrades in information security technology. For example, frequent information security technology changes and upgrades unsettle users and create uncertainty that they must constantly learn and educate themselves about new information security technology. Organizations often require employees to change their behaviors to counteract the external threat

environment; hence, employees are often hesitant to accept an organizations' requirements because of the uncertainty of security technology change.

Security-Related Challenge Techno-Stressors

Challenge stressors could be related to positive work outcomes; these stressors are perceived as beneficial and helpful to learn and accomplish work-related tasks (Cavanaugh et al., 2000; Podsakoff et al., 2007; Hargrove et al., 2013). When an individual appraises the stressor as beneficial to job tasks, the stressor is a challenge stressor; in contrast, if the stressor is perceived as hindering the job tasks, the stressor is a hindrance stressor (Hargrove et al., 2013).

There are calls and raising recognition that positive stress may exist in the technology context (Tarafdar et al., 2017). Recently, Califf et al. (2020) conceptualized a holistic technostress process that includes positive and negative components of technostress embedded in two sub-processes: the techno-eustress sub-process and the techno-distress sub-process within the context of healthcare information technology. The technostress literature suggests two distinct types of stressors: challenge and hindrance (Tarafdar et al., 2017; Califf et al., 2020). These factors are important to improve the technology characteristics and the challenge perceived by employees (Tarafdar et al., 2017). The InfoSec literature has not yet empirically identified or investigated challenge techno-stressors and their effects; therefore, in this study, it is argued that these security challenge stressors are vital and supplemented to help employees improve their security practice and strengthen the organization's digital asset protection.

When information security job resources are sufficient, organizations tend to increase their capabilities to prevent cyber threats from happening. The InfoSec literature

also has suggested emphasizing security resources available to promote and enable information security compliance and protection (Thomson & von Solms, 1998; Siponen, 2000; Herath & Rao, 2009a; Puhakainen & Siponen, 2010). Previous studies called for diversifying the field's understanding of facilitation resources in information security, considering both technological and organizational resources (Cavusoglu et al., 2005; D'Arcy et al., 2009; Herath & Rao, 2009b; Puhakainen & Siponen 2010). The security technologies were proposed as socio-technical systems, which are essentially what cyber systems built, and made up of multiple interconnected components, including technology itself, processes, and human actors (Zimmermann & Renaud, 2019). Therefore, applying the same rationale for this study, security-related techno-reliability, security technical support, SETA availability, SETA effectiveness, and security knowledge sharing challenge stressors were included as security job resources since these resources are beneficial and challenging for employees to strengthen their security knowledge and security hygiene practice. The paragraphs below explain why these factors are treated as challenge stressors.

When individuals admit that they are vulnerable to IT security threats, they are likely to use information security technology perceived as useful. A previous experimental study of endpoint web-based security software's findings suggested that users may not perceive security software directly supporting work activities. Therefore, performance security benefits may not be explicitly recognized, encouraging further research in information security technology adoption (Shropshire et al., 2015). Moreover, the security threat is perceived to be severe and avoidable. An individual will be more likely to adopt IT security solutions to address the threats by evaluating the capabilities of

such technology and form a disposition toward it (Boss et al., 2015; Johnston & Warkentin, 2010). Various security-related technostress characteristics with an appropriate amount of stress may positively affect employees' work performance, which leads to a need for recommended further study to strengthen understanding of the unique impact of security-related techno stressors (Hwang & Cha, 2018, page 290).

Security Education Training Awareness (SETA) Availability is regarded as one of the most important explicit methodologies that guide employees to achieve security goals in the workplace (Zakaria, 2006). SETA programs were found to positively influence perceived certainty and punishment severity (D'Arcy et al., 2009; Zakaria, 2006). Studies suggested organizations should consider having a budget for SETA efforts to motivate employees to strengthen information security policy compliance intention and weaken information systems misuse intention (D'Arcy et al., 2009; Herath & Rao, 2009b; Whitman et al., 2001). SETA contains security policy education and training and covers several security technology instruction guidelines. For example, employees are sometimes required to use VPN when off-site work and the need for MFA should be a part of the SETA program. These are important and continuously updated as new technology and associated security issues emerge. Training needs will shift and update employees with new skills and capabilities necessary to respond to technology changes and update and foster good security practices within organizations.

Standards bodies, such as the National Institute of Standards and Technology (NIST), industry, and scholars emphasized the vitality of effective security training and awareness programs (National Institute of Standards and Technology, 2014; Cisco, 2018; Bulgurcu et al., 2010; Siponen, 2000; Thomson & van Niekerk, 2012; Yoo et al., 2018).

Security Education Training Awareness (SETA) Effectiveness refers to security training as an important resource that positively promotes employees' security efficacy (D'Arcy et al., 2009; Herath & Rao, 2009b). When employees perceive SETA as effective, they believe they have the necessary knowledge and skills to handle security issues in the organization. People trained effectively are better equipped with knowledge and skills on security guidelines and security technology (D'Arcy et al., 2009; Herath & Rao, 2009b). Hence, SETA effectiveness is included in this study and argued that the more effective the SETA program is, the more engaging the employees will become and the more beneficial they feel about it.

Technology reliability is a way to maintain user engagement and increase individual confidence when using technology, thereby creating a positive user experience (Ayyagari et al., 2011; Califf et al., 2020). Security techno-reliability is the extent of the dependability and consistency of a security-related system, which is recognized as a factor in IS success models (DeLone & McLean, 1992; DeLone & McLean, 2003; Jiang et al., 2002). However, present-day investment in information security technology is influenced by normative pressure from the dominant players and partners that organizations must follow and invest in without adequately considering its reliability (Cavusoglu et al., 2015). Zimmermann and Renaud's (2019) "Cybersecurity, Differently" suggests that human actors with minimal security expertise should be recognized as task experts. These are those who can best describe their tasks, specific goals, the processes they engage in, and identify the factors that influence constraints.

When new information security technologies are implemented, IT professionals should encourage users to explore and provide help desk and technical support to resolve

end-user problems. Security technical support has been found positively significant in strengthening employees' self-efficacy in various technology contexts (Herath & Rao, 2009b; Siponen, 2000). Previous studies suggested that technical support also helps reduce the negative aspects of technostress (Sykes, 2015; Califf et al., 2020; Ragu-Nathan et al., 2008). Technical support was suggested to reduce regular workload during critical systems implementation and give employees time to learn and use (Brod, 1984; Ragu-Nathan et al., 2008). Hence, it is argued that security technical support can positively impact employees' positive psychological response to techno-stressors.

Information security knowledge is often embedded not solely in the documents or repositories but also organizational processes and practices. The basic security knowledge can be treated as organizational members able to perform, learn, and teach security tasks in terms of protection and reflection procedures on information security matters. Zakaria (2006) emphasized the importance of changing tacit knowledge to explicit knowledge in terms of knowledge creation, especially on security knowledge amongst employees in organizations. The emphasis is necessary because security knowledge must be externalized to share and learn from others' security practices, eventually encouraging each employee to perform, learn and teach security tasks effectively and efficiently (Safa & Von Solms, 2016). For example, colleagues who have better knowledge and experience with security technology would share the knowledge and experience with the less experienced colleagues about utilizing the MFA and VPN features or strengthening the email threat protection through email security features. Furthermore, Zimmermann and Renaud (2019) proposed the mindset manifests that

encourage employees as human-as-solution by increasing security awareness and knowledge as an essential part of information security solutions.

Distress and Eustress

Stress is a complex two-sided phenomenon, and individuals can appraise environmental conditions as both threatening and challenging, and the respective outcomes can be damaging and beneficial, respectively (Lazarus & Folkman, 1984). For example, implementing a new system can be appraised as a threat or as an opportunity, upon which different kinds of adaptation behaviors are engaged, leading to different kinds of outcomes (Beaudry & Pinsonneault, 2010; Cooper et al., 2001). A negative stress response (detrimental stress) is a particular relationship between the person and the environment that the person appraises as taxing or exceeding his or her resources and endangering his or her well-being (Lazarus & Folkman, 1984). The stress response is an evaluative process that determines why and to what extent a particular transaction or series of transactions between the person and the environment is stressful. (Lazarus & Folkman, 1984). Cognitive appraisal is an evaluative process that determines why and to what extent a particular transaction or series of transactions between the person and the environment is stressful. Previous research discussed the importance of psychological stress responses to investigate stress research (Califf et al., 2020; Cooper et al., 2001; Lazarus, 1995; Lazarus & Folkman, 1984); therefore, exploring the stressors-stress response-outcome process in the information security technology context would increase our knowledge and understanding of the transaction between the individual and the environment.

Techno distress is a sub-process in which individuals appraise security techno stressors as unfavorable or hindrance to their job goal attainment and well-being (Tarafdar et al., 2017). The security techno-distress could hinder employees' work progress. They may perceive security tech as lowering their productivity as security often makes employees feel anxiety, frustration, and anger when security techno-stressors are in place (D'Arcy et al., 2014; Posey et al., 2014). An example of security techno distress is that employees must get permission from the security department before exchanging documents with colleagues and external partners. Moreover, constant upgrades in information security technology make employees feel anxious since organizations constantly try to change their security tech to better suit the requirements of newer security tech environments, imposing stress on employees. Therefore, information security techno-distress is perceived as technology-related stress created or caused using information security technology.

Information security technology provides individual employees and consumer protection of important information assets using data encryption, firewalls, cloud computing, antivirus, anti-spyware software, and access control software. Previous study findings suggested that technical security demands more security resources from employees than managerial security since it directly controls employees during their overall work processes through technical security systems (Lee et al., 2016). Managerial security emphasizes strengthening employees' security awareness, knowledge, and behavioral information security measures, while technical security focuses on information security applications. Information security technology creates "bad" stress by posing an obstacle to task fulfillment, being a resource constraint, eliciting role or task

ambiguity, and producing role or task conflicts that all may inhibit individual learning or personal growth (Tarafdar et al., 2015; Ragu-Nathan et al., 2008).

Although psychology and organizational behavior differentiate between negative (distress) and positive stress responses (eustress), InfoSec literature primarily focuses on the negative aspects of technology-induced negative stress (D'Arcy & Teh, 2019; Hwang & Cha, 2018; Kim et al., 2016). Stressors are inherently neutral; whether they lead to a positive or negative stress response relies on an individual's cognitive appraisal and how the situation will affect well-being. Based on the JD-R model, demand from technology characteristics may create a misfit between demands and individual values, while resources such as SETA training and security technical support may buffer the negative effect (Bakker & Demerouti, 2007; Bakker & Demerouti, 2017).

Eustress is referred to as stress that creates an opportunity. It builds a positive appraisal of demands in the environment to promote personal growth and promotion. Cavanaugh et al. (2000) differentiate between challenge and hindrance stressors; their findings suggested that challenge stressors can lead to a beneficial view of stress, called eustress. This beneficial stress is called eustress (Selye, 1974). It represents a positive appraisal of demands based on the potential for the demands to result in personal benefits (Simmons & Nelson, 2001). More technology-focused, security techno-eustress explains how individuals appraise information technologies as challenging or thrilling (Tarafdar et al., 2017; Tarafdar et al., 2010). Similar logic can be applied to information security technology as employees may perceive security technology as interesting and motivating to practice their security hygiene. For instance, companies may strengthen employees' understanding of information security technology through their security education

training program and encourage them to watch or attend information security technology training with the IT department.

Techno-eustress has been defined as “the phenomenon that embodies the positive stress that individuals face in their use of IS” and occurs when “individuals appraise IS as challenging or thrilling” (Tarafdar et al., 2017, pg. 14). Eustress may suggest end-users think they have control over the information security technology. A sense of being in a challenging position helps them feel secure and stabilizes their emotional state. For instance, an online banking user who frequently changes passwords updates antivirus and anti-spyware software, and installs security patches for his/her operating systems will have a positive emotion and not feel distressed by losing identity in online transactions. Alternatively, an employee in the education industry is required to install an employer-supplied VPN at home, s/he may perceive VPN as helping to protect the organizational data assets, and s/he could feel excited to install VPN to secure his data on his/her computers at home. With confidence and encouragement, users will be more motivated to take security actions to counter the security stress. A previous study developed a web-based security tool to assess PCs’ susceptibility to attacks from third parties and reported results to end-users via PHP-generated webpage content, helping end-users stay vigilance (Shropshire et al., 2015). Security software benefits often go mostly unnoticed.

In this study, security techno-eustress is defined as the phenomenon associated with a positive stress response that individuals experience while using information security technology (Tarafdar et al., 2017). Individuals may perceive information security technologies as beneficial to learn new skills and strengthen individual security awareness. Individuals may perceive information security technologies functionality as

an opportunity for innovative use to evaluate security characteristics such as reliability as opportunities to experiment and use to enhance their information security good practice behavior. For example, employees may stop using USB thumb-drive to back up data and gradually adopt cloud-based security to protect their digital assets. Furthermore, employees may utilize features (i.e., secured file storage, encryption protocols, sites breach alerts) on a password manager to adhere to the organization's stringent password policy instead of writing passwords down on the sticky note.

Security Counterproductive Behavior

Counterproductive behavior is defined as a set of distinct acts that share the characteristics of negative and harmful to organizations and organization stakeholders (Spector & Fox, 2005). Although counterproductive behavior is intended to have a detrimental effect on organizations and individuals, it was conceptualized in various ways, including organization aggression (Neuman & Baron, 1998; Fox & Spector, 1999), deviance (Hollinger, 1986; Robinson & Bennett, 1995). Counterproductive behaviors were associated with a general disregard for organizational safety and policies (Spector et al., 2006; Spector & Fox, 2010). In addition, these volitional behaviors are associated with actions that may be deemed accidental or directly mandated as a behavioral manifestation of job stress (Fox et al., 2011; Spector & Fox, 2005). These counterproductive behaviors were operationalized as the multidimensional construct to capture and explain more specific negative behaviors within the workplace, including sabotage, withdrawal, production deviance, theft, and abuse (Spector et al., 2006).

InfoSec literature proposed two distinct instruments of information security deviant behaviors, including resource misuse and security carelessness (Chu & Chau,

2014). Information security deviant behavior is defined as the voluntary behavior of employees within organizations that differ markedly from the organizations' information security norms and that other employees normally consider to be wrong (Chu & Chau, 2014). While security carelessness refers to the behavior of not giving sufficient thought or attention to individual actions in using or handling IS resources. In contrast, resource misuse refers to behaviors relating to inappropriate or improper use of IS resources in employees' daily work activities.

Recently, a study attempted to develop another third behavior used to explain and assess employees' non-malicious information security behavior, called security procrastination (Ifinedo, 2019). Security procrastination refers to employees procrastinating in carrying out required IS actions. It is a behavior of putting off or delaying IS activities requiring immediate attention. The reasoning suggests that when employees postpone responsibilities, decisions, and duties in updating IS security tasks may lead to security-related problems for their organizations.

In this study, counterproductive security behavior is defined as abnormal behaviors by employees who do not follow the organization's information security norms, yet without bad intention to damage the organization's digital assets. Also, an individual's behavior in organizations was suggested to be influenced by stress; therefore, it is arguable that these counterproductive security behaviors can be caused by job stressors (Chen & Spector, 1992; Fox et al., 2001; Fox et al., 2012). Table 2.1 contains the definitions of all constructs used in the study.

Table 2.1

Definitions and Constructs Used in Study

Construct	Operational Definitions	Reference
Security techno-overload	The degree of increase in the amount of workload due to required information security technology.	Hwang and Cha, 2018
Security techno-complexity	The degree of complexity of information security technology, associated with information security technology that makes employees feel incompetent.	Hwang and Cha, 2018
Security techno-uncertainty	The degree of constant upgrades in information security technology that affect individual work-related tasks.	Hwang and Cha, 2018
SETA Availability	The degree of deterrent effect that could be achieved through ongoing security briefings or courses that reinforce acceptable usage guideline and emphasize potential consequences for misuse.	D'Arcy et al., 2009
SETA Effectiveness	The extent to which employees attending the SETA programs feel that they achieve the goal of SETA effectively	Yoo et al., 2018
Security techno-reliability	The extend of dependability and consistency of the information security technology's features	Ayyagari et al., 2011
Security technical support	The extent of support activities to end-users and responsiveness addressing information security-related problems from IT help desk.	Liang and Xue, 2010; Tarafdar et al., 2014
Knowledge Sharing	The extent of knowledge sharing about information security technology within organization to increase awareness and mitigate the risk of information security incidents.	Extended and adapted from Ragu-Nathan, 2008
Security Techno-Distress	The perception of negative stress response toward information security techno stressors that affect individual's well-being and goal accomplishment.	O'Sullivan, 2011
Security Techno-Eustress	The perception of positive stress response toward information security techno stressors that benefit individual's learning and personal growth.	Selye, 1974; Tarafdar et al., 2017
Security Counterproductive behavior	The abnormal behaviors engaged in by employees who do not follow the organization's information security norms, yet without bad intention to damage the organization's digital assets	Chu and Chau, 2014; Ifinedo, 2019

Research Model and Hypotheses

In this section, the JD-R integrated with the technostress trifecta frameworks is discussed to develop hypotheses for this study. Job demands refer to “physical, social, or organizational aspects of the job that require sustained physical or mental effort and are therefore associated with certain psychological costs” such as exhaustion (Demerouti et al., 2001, page 501). Job demands are positively related to exhaustion (Bakker & Demerouti, 2007; Crawford et al., 2010). Hindrance stressors are considered constraints or barriers since they affect individuals’ job-related task accomplishment and personal growth (Cavanaugh et al., 2001; Podsakoff et al., 2007; Demerouti & Bakker, 2011). Examples of hindrance stressors are role ambiguity, organizational politics, interpersonal conflict, and role conflict (Cavanaugh et al., 2001; Demerouti & Bakker, 2011; LePine et al., 2004). These stressors are considered as ‘bad’ demands (Demerouti & Bakker, 2011) and associated positively with negative psychological and organizational outcomes, including turnover intention, absenteeism, tardiness, work performance, job satisfaction, and organizational commitment (LePine et al., 2004; LePine et al., 2005; Podsakoff et al., 2007). JD-R theory guides understanding the effects of information security technology demands taxing on employees. The effects of security demands exhibit themselves in physical, social, and organizational aspects that affect employees’ work performance and well-being.

The JD-R framework is characterized by its flexibility in operationalizing all job demands and resources specific to a certain context and environment (Pham et al., 2016; LePine et al., 2005; Demerouti & Bakker, 2001; Schaufeli, 2017). Furthermore, job demands were operationalized as a second-order construct containing first-order

constructs, such as workload, complexity, time pressure, administrative stressors (Crawford et al., 2010; Demerouti & Bakker, 2001; Schaufeli, 2017; Wolter et al., 2018). In the InfoSec literature, previous studies show that security-related stressors (uncertainty, complexity, and overload) have a positive relationship with negative psychological stress responses, employees' emotions of frustration and fatigue, which consequentially increase neutralization, noncompliance intention, and decrease compliance behavior (D'Arcy et al., 2014; D'Arcy et al., 2018; D'Arcy & Teh, 2019; Zhen et al., 2021). Moreover, qualitative findings found that employees have been stressed with complex security requirements, with slim opportunities to develop a hands-on experience or adapt security into their work routines (Posey et al., 2014). In this study, the security job demands, namely, hindrance security techno-stressors, include security techno-overload, security techno-uncertainty, and security techno-complexity. These have been associated with negative psychological stress responses due to information security technology getting more complex and specialized, making employees' working environment susceptible to technostress and resultant role stress that affect overwhelming stress on employees (D'Arcy & Teh, 2019; Hwang & Cha, 2018). The information security technologies' demands occur on top of employees' work-related tasks. For instance, employees are often required to change passwords and recall complex passwords for various accounts or create email encryption with external stakeholders while dealing with urgent requests from clients. The imposition of information security technologies causes employees to be overwhelmed and are perceived as laborious (D'Arcy et al., 2014; Posey et al., 2011; Posey et al., 2014; Puhakainen et al., 2010; Wall, 2011). Moreover, security technologies uncertainty occurs when employees may not

know what to do or whom to ask for help. Technical security requirements (i.e., email encryption) or infinite technology upgrades hinder employees from developing an experiential basis and constantly refreshing their knowledge. Hence, employees face high-security standards and diverse security technology. The convenience of employees' daily work is inevitably affected, resulting in negative stress responses regarding the organization's security technology guidelines.

The overarching stress process contains two sub-processes associated with the positive and negative stress responses, namely eustress and distress, depending on whether the stressor is perceived as beneficial or harmful. (Califf et al., 2020; Hargrove et al., 2015; Simmons & Nelson, 2007; Sommer et al., 2016). Hindrance stressors are negatively associated with negative emotional stress responses and detrimental psychological and behavioral outcomes. They stimulate negative emotions because of negative appraisal hindering personal growth and goal attainment. At the same time, they have a negative relationship with positive attitudinal and behavioral outcomes, including engagement, attentiveness, and organizational citizenship behavior (Crawford et al., 2010; Rodell & Judge, 2009). Therefore, in this study, security technology hindrance stressors, namely security job demands, was argued to be positively associated with negative stress response and represent a threat because they are viewed as deterrents to achieving positive outcomes. Therefore, I hypothesized as follow:

H1a: Security job demands is positively associated with security techno-distress

H1b: Security job demands is negatively associated with security techno-eustress

JD-R focuses on two job-related factors that predict employee response, including demands and resources (Bakker & Demerouti, 2007), assuming that when an individual

has sufficient helpful resources to rely on, it will reduce their experience with distress. Job resources are physical, psychological, social, or organizational aspects of the job that are perceived as instrumental to personal development, achieving work goals (Demerouti et al., 2001). Also, the presence of these resources should serve to reduce distress by allowing workers to complete tasks without seeking additional resources. According to the JD-R framework, job resources were operationalized as a second-order construct that contains various first-order factors, including role clarity, supervisor support, job security, team effectiveness (Crawford et al., 2010; Demerouti & Bakker, 2001; Schaufeli, 2017; Wolter et al., 2018). In addition, job resources should increase eustress by providing the resources employees need to pursue their jobs' vital aspects (Schaufeli & Bakker, 2004). Furthermore, challenge stressors promote personal growth and achievement, often perceived as beneficial (Cavanaugh et al., 2001; Podsakoff et al., 2007; Demerouti & Bakker, 2011). Examples of challenging stressors were workload, responsibility (Cavanaugh et al., 2001; Demerouti & Bakker, 2011; LePine et al., 2005). In IS, the challenge techno-stressors were usefulness, technical support, and involvement facilitation (Califf et al., 2020). These challenge stressors are considered good resources and associated positively with job satisfaction, organizational commitment, and job performance (Califf et al., 2020; Ragu-Nathan et al., 2008; Tarafdar et al., 2010).

Reliability is one of the major IS characteristics recognized in the IS success model (Delone & McLean, 1992; Jiang et al., 2002; Tarafdar et al., 2017). Technology reliability is a way to maintain user engagement and increase individual confidence when using technology, thereby creating a positive user experience (Ayyagari et al., 2011; Califf et al., 2020). Therefore, it is argued that security techno reliability is one of the

critical characteristics of an indispensable resource. Moreover, previous studies examined and suggested that technical support can inhibit detrimental stress and help to reduce the negative techno stressors (Syke, 2015; Califf et al., 2020; Ragu-Nathan et al., 2008). When new information security technology is implemented, IT professionals should encourage users to explore and provide help desk and security technical support to resolve end-user problems. Technical support was suggested to reduce regular workload during critical systems implementation and give employees time to learn and use (Brod, 1984; Ragu-Nathan et al., 2008). In addition, security education and training (SETA) are one of the essential resources that firms need to have in place to strengthen appropriate IS usage and educate employees on potential consequences of misuse (D'Arcy et al., 2009; Herath & Rao, 2009; Hwang et al., 2019; Whitman et al., 2001). SETA Availability is the degree of achievable deterrent effect through ongoing security briefings or courses that reinforce acceptable usage guidelines and emphasize potential misuse consequences (D'Arcy et al., 2009; Zakaria, 2006). However, SETA cannot be "one size fits all" due to not taking into account individual motivations and appraisals, especially in the rapidly changing information security technology because cyber attackers are determined to make novel attack techniques (Zimmermann & Renaud, 2019). Organizations need to provide effective security training that supports and strengthens security awareness and improves employees' security compliance (Yoo et al., 2018). As a result, SETA effectiveness is defined as employees' feeling from training that they achieve the goal of SETA effectively. Knowledge sharing is an important growth factor within the current organizational environment (Ragu-Nathan et al., 2008). Due to the ever-increasing sophistication of information security technology and cyber threats, security knowledge

sharing is needed to raise awareness and know-how to avoid cyber threats and mitigate their risks. Also, it is important to involve employees across all departments to participate in the information security technology design to help understand their needs (Califf et al., 2020; Safa & Von Solms, 2016; Tarafdar et al., 2010; Zakaria, 2006).

Organizations provide adequate information systems resources and guidelines to help employees reduce burnout and strengthen their information security best practice (D'Arcy et al., 2009; Pham et al., 2016; Pham et al., 2019). Job resources have been positively related to work motivation, organizational commitment, and engagement (Bakker et al., 2003). Applying a similar rationale, it is argued that when security job resources are provided, that should strengthen employees' positive psychological response and weaken their negative psychological response. Therefore, the following hypotheses are formed.

H2a: Security job resources (challenge stressors) is negatively associated with security techno-distress

H2b: Security job resources (challenge stressors) is positively associated with security techno-eustress

Counterproductive behavior has been operationalized as a multi-dimensional construct with a second-order construct to capture and explain more specific behaviors within the workplace, including sabotage, withdrawal, production deviance, theft, and abuse (Spector et al., 2006). In this study, counterproductive security behavior that comprises behavioral manifestations is operationalized with three unique instruments: resource misuse, security procrastination, and security carelessness developed and validated (Chu & Chau, 2014; Ifinedo, 2019). Previous information security studies

suggested that positive and negative psychological responses may influence cybersecurity workers on their level of readiness and responsiveness against cyber threats (Helkala, 2016). In contrast, cybersecurity workers may have a positive psychological response if adequate security resources are offered (Helkala, 2016; Lundgren & Bergstrom, 2019). Following (Califf et al., 2020; Tarafdar et al., 2017) propositions on designing IS to aid in challenge and threat coping responses and designing IS to enhance positive outcomes and diminish adverse effects.

Strain is defined as the behavioral, psychological, and physiological outcomes of stress observed in individuals (Cooper et al., 2001). Techno stressors are associated with negative psychological and behavioral strains (Ayyagari et al., 2011; Cooper et al., 2001; Tarafdar et al., 2010). Psychological strains are emotional reactions to stressor conditions and include, among others, dissatisfaction with the job, depression, and negative self-evaluation. Strain is the outcome of stress and results from distress and is adverse consequences emerging from a direct relationship with various techno stressors (Tarafdar et al., 2015; Tarafdar et al., 2017). Simultaneously, behavioral outcomes included reduced productivity, increased turnover and absenteeism, and poor performance (Cooper et al., 2001; Tarafdar et al., 2007). Furthermore, there is an adverse effect of ICT techno stressors on users' job satisfaction and performance (Ragu-Nathan et al., 2008; Tarafdar et al., 2010). Therefore, it is argued that the behavioral strain, namely security counterproductive behavior, is the adverse outcome from the security technology's psychological responses (Figure 2.1).

Hence, in this study, the following hypotheses were formed:

H3: Security techno-distress is positively associated with security counterproductive behaviors

H4: Security techno-eustress is negatively associated with security counterproductive behaviors

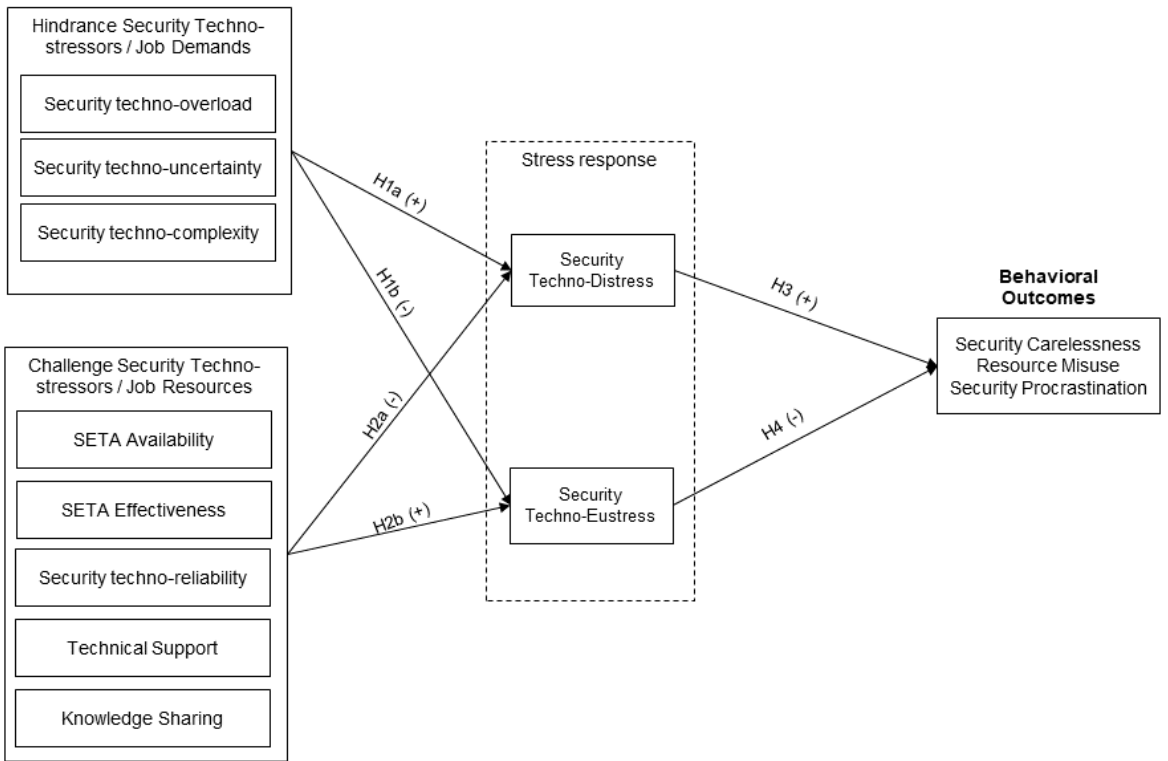


Figure 2.1: *Conceptual Framework*

CHAPTER 3

RESEARCH METHODOLOGY

General Approach

A quantitative survey using a survey panel design was conducted. Scale measurements that reflect the constructs discussed in Chapter 2 were adapted and extended from previous studies. The partial least squares (PLS) methodology was applied to empirically test the model (Chin, 1998; Hair et al. 2014)

The university human use committee approved the study. Target subjects were adult employed individuals who use information technology in their daily work activities. Appropriate respondents were asked two screening questions designed to check whether they use information technology to perform their work and whether they are aware of information security technology in place in their organization (see Appendix B). Participants who were qualified were allowed to complete the survey using Qualtrics web-based survey software.

Participants were required to live in the United States to control for cultural biases in our sample. Incomplete data sets and low survey completion times were controlled to guarantee high data quality further. Besides, the survey included quality control questions and poor data from respondents who failed to pay attention or gave nonsense answers to open-ended questions were eliminated. A cross-sectional correlational design was adopted to understand the relationship between the predictors and outcome variables.

There are several reasons why online panels are appropriate for distributing the survey to the target population sample. First, online panels allow data collection from a large population of respondents (Steelman et al., 2015). Second, online research panels provide respondents with different backgrounds and experiences. Third, the screening options allow us to approach respondents who properly fit our research (Lowry et al., 2016). Finally, online panels provide built-in anonymity and feature to ensure data quality (Rouse, 2015). Amazon.com's Mechanical Turk (MTurk) was used in this study. MTurk is a unique source of online panel data to access to employees at diverse organizations, which is no longer an exception in scientific research (Owens & Hawkins, 2019). MTurk provides higher generalizability on the pilot and exploratory studies and has greater potential for cross-validation and generalization testing of data because data collected via Mechanical Turk are recommended with externally and internally valid (Berinsky et al., 2012; Lowry et al., 2016). In addition, rigorous criteria were set to increase the data quality; criteria settings were placed that only accepted MTurk users to participate in the study if and only if they had more than 5,000 Human Intelligence Tasks (HIT) approved, 98% HIT approval rate. They were located in the United States.

Measures

We adapted existing validated well-tested measurement items in the extant literature. The first-order measures, including security techno-overload, security techno-uncertainty, and security techno-complexity, are from (Hwang & Cha, 2018). The measurement of SETA effectiveness was adopted from Yoo et al. (2018), SETA availability was adopted from D'Arcy et al. (2009); Sarkar et al. (2020), security

techno-reliability from Ayyagari et al. (2011), security technical support from Liang and Xue (2010) and Tarafdar et al. (2014), and security knowledge sharing was self-developed in this study. Security technology negative psychological response (security techno-distress) was taken and adapted from Cohen et al. (1983), Watson et al. (1988), and Xu et al. (2019), while security technology positive psychological response (security techno-eustress) was adapted from O'Sullivan (2011) and Watson et al. (1988). Security counterproductive behaviors, including security carelessness, security procrastination, and information systems resource misuse, were adapted and extended (Chu & Chau, 2014; Ifinedo, 2019). A 7-point Likert response scale, using anchor text for all seven levels, was used for overload, uncertainty, complexity, SETA effectiveness, SETA availability, security techno-reliability, security technical support, and knowledge sharing (1-strongly disagree to 7-strongly agree). A 7-point Likert response scale, using anchor text for all seven levels, was used for distress and eustress (1-Never to 7-Always) and was used for security carelessness, resource misuse, and security procrastination. A bipolar 7-points scale was used for a control variable, self-efficacy (Very difficult to very easy). Table 3.1 contains the constructs' measurement items and sources.

Job demands were conceptualized as a formative second-order latent variable consisting of security techno-overload, techno-uncertainty, and techno-complexity. Similarly, job resources were treated as a formative second-order latent variable composed of SETA availability, SETA effectiveness, security techno-reliability, technical support, and knowledge sharing. Behavioral outcomes were conceptualized as a formative second-order latent variable comprised of security carelessness, resource misuse, and security procrastination.

In addition, this study attempted to uncover the control variables recommended by (Hwang & Cha, 2018; Tarafdar et al., 2011; Tarafdar et al., 2017). Control variables consisted of gender, age, education, year of work experience, security self-efficacy, educational level, occupation, organizational tenure, and job role (IT and non-IT).

Table 3.1

Constructs, Adapted Items, and Sources

Items	Construct	Reference
STO1 STO2 STO3 STO4 STO5	<p>Security techno-overload</p> <p>I am forced by my organization's information security technology to work much faster in order to complete my work.</p> <p>I am forced by information security technology to do more work than I can handle.</p> <p>I am forced by information security technology to work with very tight schedules.</p> <p>I take too much care of my data protection on information security technology.</p> <p>Because of my organization's information security technology, I have to work faster to complete my work on time.</p>	Hwang and Cha (2018)
STU1 STU2 STU3	<p>Security techno-uncertainty</p> <p>There are always new developments in the information security technology we use in our organization.</p> <p>There are frequent upgrades to the information security technology in my organization.</p> <p>There are always new information security technology requirements in my job.</p>	(Hwang and Cha 2018)

Items	Construct	Reference
STC1 STC2 STC3	<p>Security techno-complexity</p> <p>I need a long time to understand and use new information security technology</p> <p>I do not find enough time to upgrade my information security technology skills.</p> <p>I often find it too complex to understand and use new information security technology</p>	
STR1 STR2 STR3	<p>Security techno-reliability</p> <p>The features provided by my organization's information security technology are dependable.</p> <p>The capabilities provided by my organization's information security technology are reliable.</p> <p>My organization's information security technology behave in a consistent way.</p>	(Ayyagari et al. 2011)
TS1 TS2 TS3 TS4	<p>Security technical support</p> <p>Our IT Support team does a good job of answering questions regarding information security technology.</p> <p>Our IT Support team is staffed by knowledgeable individuals about information security technology.</p> <p>When I have a question about information security technology, our IT Support team is easily accessible.</p> <p>When I have a question about information security technology, our IT Support team is responsive to requests.</p>	(Liang and Xue 2010)
SETA1 SETA2 SETA3 SETA4 SETA5	<p>SETA availability</p> <p>My organization provides training to help me improve my awareness of information system security issues.</p> <p>My organization provides me with education on information security technology use.</p> <p>In my organization, I am briefed on the consequences of modifying computerized data in an unauthorized way.</p> <p>My organization educates me on my information security technology responsibilities.</p> <p>In my organization, I am briefed on the consequences of accessing information systems that I am not authorized to use.</p>	(D'Arcy and Hovav 2009)

Items	Construct	Reference
SETE1 SETE2 SETE3 SETE4	<p>SETA effectiveness</p> <p>My organization's security education training increases my knowledge on information security issues.</p> <p>I understand the basic ideas of the security knowledge taught in security training.</p> <p>I try to apply the security knowledge I gained in information security technology training.</p> <p>My organization's security training motivates me to integrate the security knowledge learned into my work.</p>	(Yoo et al. 2018)
KS1 KS2 KS3	<p>Security knowledge sharing</p> <p>My organization encourages knowledge sharing to help deal with new threats associated with information security technology.</p> <p>My organization emphasizes teamwork in dealing with new information security technology problems.</p> <p>In my organization, people are encouraged to help each other when facing information security technology problems.</p>	Self-developed
Dist1 Dist2 Dist3 Dist4 Dist5	<p>Security techno distress</p> <p>How often have you been upset because of something that happened unexpectedly with information security technology while you are working?</p> <p>How often have you felt that you were unable to control the important things related to dealing with information security technology?</p> <p>How often have you felt that difficulties related to information security technology were piling up so high that you could not overcome them?</p> <p>While dealing with information security technology for your work tasks, how often have you felt nervous and stressed?</p> <p>When encountering information security technology issue while doing your work, how often have you found that you could not cope with all of the things that you had to do?</p>	(Cohen et al. 1983)

Items	Construct	Reference
<p>Eus1</p> <p>Eus2</p> <p>Eus3</p> <p>Eus4</p> <p>Eus5</p> <p>Eus6</p>	<p>Security techno eustress</p> <p>How often do you effectively cope with stressful changes that occur due to information security technology uncertainty?</p> <p>How often do you deal successfully with irritating information security technology hassles?</p> <p>In general, how often do you feel motivated by your stress related to information security technology?</p> <p>In general, how often are you able to successfully control the irritations in your work associated with information security technology and threats?</p> <p>When faced with information security technology stress, how often do you find that the pressure makes you more productive?</p> <p>How often do you feel that you perform better on a work task when under information security pressure?</p>	<p>(O’Sullivan 2011)</p>
<p>SC1</p> <p>SC2</p> <p>SC3</p> <p>SC4</p> <p>SC5</p>	<p>Security carelessness</p> <p>Not always treating sensitive data carefully.</p> <p>Not checking sources when install new mobile apps for work purpose.</p> <p>Using public Wi-Fi to access or transmit work-related data.</p> <p>Using work cloud-storage to store personal data.</p> <p>Pasting or sticking passwords on office desks and other locations.</p>	<p>(Chu and Chau 2014; Ifinedo 2019)</p>
<p>RM1</p> <p>RM2</p> <p>RM3</p> <p>RM4</p> <p>RM5</p>	<p>IS resource misuse</p> <p>Visiting nonrelated websites at work.</p> <p>Downloading unauthorized software onto work devices (e.g. computer, smartphone).</p> <p>Not logging out of secure system after use.</p> <p>Leaving one’s work laptop unattended.</p> <p>Allowing others (e.g. family) to play with work laptop or work devices.</p>	<p>(Chu and Chau 2014; Ifinedo 2019)</p>

Items	Construct	Reference
SP1 SP2 SP3 SP4	Security procrastination Not updating passwords on work devices. Not updating passwords on work software. Not updating work-related passwords regularly. Not backing up data file frequently.	

Pilot Test

The purpose of the pilot test was to make a final check on the quality of the scale measurement items to assess any issues with the instrument to check for any potential internal validity issues prior to moving forward with the actual study. In addition to using previously validated questions, all measures were pretested and modified by two business professors with expertise in survey research and three professionals with information security technology experience. The pilot study data were used to check scale reliability; it was not used in subsequent data analysis.

Pilot Test Reliability Analysis

Most of the scales were reliable because Cronbach's alpha values were above 0.7, which passed the suggested threshold for reliability (Fornell & Larcker, 1981). However, Cronbach's alpha values of security techno-uncertainty, technical support, and eustress are below 0.7 (See Table 3.2).

Table 3.2

Cronbach's Alpha Values of Security Techno-Uncertainty, Technical Support, and Eustress

Scale	Cronbach's alpha	Composite Reliability	AVE
Security techno-overload	0.687	0.916	0.687
Security techno-uncertainty	0.485	0.686	0.473
Security techno-complexity	0.844	0.902	0.761
SETA Availability	0.682	0.792	0.437
SETA Effectiveness	0.766	0.847	0.582
Security techno-reliability	0.749	0.916	0.687
Technical Support	0.536	0.744	0.427
Distress	0.929	0.946	0.780
Eustress	0.806	0.832	0.483
Carelessness	0.691	0.953	0.745
Misuse	0.904	0.928	0.722
Procrastination	0.918	0.939	0.753

Therefore, new items were extended and developed for the latent variables of security techno-uncertainty and security technical support. At the same time, the eustress's outer loadings were evaluated to improve the average variance extracted (AVE) in the actual data collection. The finalized version of the revised measurement is in Table 3.3.

Table 3.3

Measurement of Outer Loadings of the Eustress

Items	Construct	Reference
STO1	Security techno-overload I am forced by my organization's information security technology to work much faster in order to complete my work.	Hwang and Cha (2018)
STO2	I am forced by information security technology to do more work than I can handle.	
STO3	I am forced by information security technology to work with very tight schedules.	
STO4	I take too much care of my data protection on information security technology.	
STO5	Because of my organization's information security technology, I have to work faster to complete my work on time.	
STU1	Security techno-uncertainty There are always new developments in the information security technology we use in our organization.	(Hwang and Cha 2018)
STU2	There are frequent upgrades to the information security technology in my organization.	
STU3	There are always new information security technology requirements in my job.	
STU4_new	My organization always notifies of upgrades for the information security technology. (extended)	
STC1	Security techno-complexity I need a long time to understand and use new information security technology.	
STC2	I do not find enough time to upgrade my information security technology skills.	
STC3	I often find it too complex to understand and use new information security technology.	

Items	Construct	Reference
STR1 STR2 STR3 STR4_new	<p>Security techno-reliability</p> <p>The features provided by my organization's information security technology are dependable.</p> <p>The capabilities provided by my organization's information security technology are reliable.</p> <p>My organization's information security technology behaves in a consistent way.</p> <p>My organization uses dependable information security technology.</p>	(Ayyagari et al. 2011)
TS1 TS2 TS3 TS4	<p>Technical Support</p> <p>Our IT Support team does a good job of answering questions regarding information security technology.</p> <p>Our IT Support team is staffed by knowledgeable individuals about information security technology.</p> <p>When I have a question about information security technology, our IT Support team is easily accessible.</p> <p>When I have a question about information security technology, our IT Support team is responsive to requests.</p>	(Liang and Xue 2010)
SETA1 SETA2 SETA3 SETA4 SETA5	<p>SETA Availability</p> <p>My organization provides training to help me improve my awareness of information system security issues.</p> <p>My organization provides me with education on information security technology use.</p> <p>In my organization, I am briefed on the consequences of modifying computerized data in an unauthorized way.</p> <p>My organization educates me on my information security technology responsibilities.</p> <p>In my organization, I am briefed on the consequences of accessing information systems that I am not authorized to use.</p>	(D'Arcy and Hovav 2009)

Items	Construct	Reference
SETE1 SETE2 SETE3 SETE4	<p>SETA Effectiveness</p> <p>My organization's security education training increases my knowledge on information security issues.</p> <p>I understand the basic ideas of the security knowledge taught in security training.</p> <p>I try to apply the security knowledge I gained in information security technology training.</p> <p>My organization's security training motivates me to integrate the security knowledge learned into my work.</p>	(Yoo et al. 2018)
KS1 KS2 KS3	<p>Knowledge Sharing</p> <p>My organization encourages knowledge sharing to help deal with new threats associated with information security technology.</p> <p>My organization emphasizes teamwork in dealing with new information security technology problems.</p> <p>In my organization, people are encouraged to help each other when facing information security technology problems.</p>	Self-developed
Dist1 Dist2 Dist3 Dist4 Dist5	<p>Security techno-distress</p> <p>How often have you been upset because of something that happened unexpectedly with information security technology while you are working?</p> <p>How often have you felt that you were unable to control the important things related to dealing with information security technology?</p> <p>How often have you felt that difficulties related to information security technology were piling up so high that you could not overcome them?</p> <p>While dealing with information security technology for your work tasks, how often have you felt nervous and stressed?</p> <p>When encountering information security technology issue while doing your work, how often have you found that you could not cope with all of the things that you had to do?</p>	(Cohen et al. 1983)

Items	Construct	Reference
<p>Eus1</p> <p>Eus2</p> <p>Eus3</p> <p>Eus4</p> <p>Eus5</p> <p>Eus6</p> <p>Eus7_new</p>	<p>Security techno-eustress</p> <p>How often do you effectively cope with stressful changes that occur due to information security technology uncertainty?</p> <p>How often do you deal successfully with irritating information security technology hassles?</p> <p>In general, how often do you feel motivated by your stress related to information security technology?</p> <p>In general, how often are you able to successfully control the irritations in your work associated with information security technology and threats?</p> <p>When faced with information security technology stress, how often do you find that the pressure makes you more productive?</p> <p>How often do you feel that you perform better on a work task when under information security pressure?</p> <p>How often do you feel that stress from information security technology has a positive effect on the results of your work? (extended)</p>	<p>(O’Sullivan 2011)</p>
<p>SC1</p> <p>SC2</p> <p>SC3</p> <p>SC4</p> <p>SC5</p> <p>SC6</p>	<p>Security Carelessness</p> <p>Not always treating sensitive data carefully.</p> <p>Not checking sources when install new mobile apps for work purpose.</p> <p>Using public Wi-Fi to access or transmit work-related data.</p> <p>Using work cloud-storage to store personal data.</p> <p>Pasting or sticking passwords on office desks and other locations.</p> <p>Not always treating sensitive data carefully.</p>	<p>(Chu and Chau 2014; Ifinedo 2019)</p>
<p>RM1</p> <p>RM2</p> <p>RM3</p> <p>RM4</p> <p>RM5</p>	<p>IS Resources Misuse</p> <p>Visiting nonrelated websites at work.</p> <p>Downloading unauthorized software onto work devices (e.g. computer, smartphone).</p> <p>Not logging out of secure system after use.</p> <p>Leaving one’s work laptop unattended.</p> <p>Allowing others (e.g. family) to play with work laptop or smart devices.</p>	

Items	Construct	Reference
	Security Procrastination	
SP1_new	Not updating mobile apps for work purpose.	
SP2	Not updating passwords on work devices.	
SP3	Not updating passwords on work software.	
SP4	Not updating work-related passwords regularly.	
SP5	Not backing up data file frequently.	

Power Analysis

A power analysis was evaluated to determine the minimum number of samples necessary for the study. Using the statistical test of linear multiple regression model with R^2 deviation from zero, G*Power 3.1 analysis was utilized to obtain a sufficient sample size, estimating the sample size based on alpha level ($\alpha = 0.01$), power ($1 - \beta = 0.95$), and a medium effect size ($f^2 = 1$) (see Appendix E), with predictor variables within the model (Hair et al., 2014). The result from the power analysis suggested that the minimum adequate sample size for this study was 236; however, the actual dataset was 549. Moreover, following the rule of thumb 10 times the largest number of structural paths directed at a particular construct in the structural model, offers a rough guideline for minimum sample size requirement (Hair et al., 2011; Marcoulides & Chin, 2013).

Actual Data Collection Procedures

It was important to prepare targeted participants with specific criteria on MTurk to identify qualified participants for this study. Recent studies have emphasized that Mturk panel is more diverse than individuals identified through traditional data sampling techniques used in most behavioral research and would thus better generalize to the general population than the previous sample techniques (Lowry et al., 2016; Steelman et

al., 2015). Therefore, a few questions were published via a human intelligence task (HIT) to assign the custom qualification criteria. Appendix D shows the requirements for participating in the survey.

In order to increase the data quality, criteria settings were placed that only accepted Mturk panels to participate in the study if and only if they had more than 5,000 Human Intelligence Tasks (HIT) approved, 98% HIT approval rate. They were located in the United States. Each response included the worker ID of the participant, which was used to assign the worker who meets the criteria to custom qualification. Workers' ID was important to identify (a) qualified to participate and (b) who participated in the pilot study so they would not be invited to participate in the actual study. Potential participants were directed to click on our survey link to read a consent form describing the research and then decide whether to proceed with the survey. There were two screening questions, asking whether there is an information security policy at their organization and whether they use technological devices to perform their works (Appendix C). Only participants who qualified for both these two conditions for their job duties at the workplace will participate in the questionnaire.

In addition, there are several quality check questions mixed within the online questionnaire, asking respondents to select a specific response if they are attentively reading the question. If their answers to quality check questions were incorrect, the survey terminated with a notice message, and the response was discarded. In addition, further calculation of the mean (average) response time of 590 participants resulted in a mean of eight minutes. Respondents' response time of fewer than eight minutes was checked and eliminated from the analysis. Moreover, several open-end questions were

asked about respondents' years of experience and current position tenure to strengthen the response quality and check if their responses were attentive and prudent.

Only qualified participants were accepted for the actual study. Among the 590 participants, 548 met the quality criteria, almost 93% of the employees surveyed. They were an adult employee who depend on information technology devices (i.e. laptop, desktop, smartphone, etc.) to do their work and their organizations have information security policy in effect.

CHAPTER 4

DATA ANALYSIS

There are two widely applied Structural Equation Modeling (SEM) techniques, namely Component-based SEM (commonly called PLS-SEM) and Covariance-based SEM. These two SEM techniques are different in term of their philosophies, distribution assumptions, and estimation objectives (Gefen et al., 2011). The partial least squares (PLS) methodology was applied to empirically test the model (Chin 1998).

PLS-SEM is an appropriate method in this research because (1) this study seeks to predict the associations among constructs in a complex research model, and also to build a theory in the context of information security technology, (2) the research model's data origin is survey data of 548 which exceeds the minimum sample requirements of PLS (Hair et al., 2014, pg. 20). There are two advantages of using PLS-SEM in this study. First, PLS offers flexibility in evaluating a structural and measurement model where relationships have not been fully examined (Chin, 1998; Gefen et al., 2000; Hair et al., 2014). Second, PLS can be applied when investigating a complex research model with many constructs and indicators (Hair et al., 2014). Finally, PLS is able to handle both reflective and formative latent variables (Lowry & Gaskin, 2014).

Descriptive Statistics

Table 4.1 shows demographics. The 548 participants' ages ranged from 20 to 73 years, with a mean of 39.34 years (standard deviation = 11.05). Of the participants, 52.7% (289) were male, and 47.3 % (259) were female. Two-thirds of the participants (66.2%) at least had a two-year college degree or higher. There are 53.8% information technology professional and 46.2% are end-user.

Table 4.1

Demographics

Subjects (n = 548)		
Characteristic	Mean/Frequency	Standard Deviation
Age	39.34	11.05
Gender	Male = 289 (52.7%) Female = 259 (47.3%)	
Education	High school = 38 (6.9%) Two-year college = 60 (10.9%) Bachelor's = 303 (55.3%) Master's = 130 (23.7%) Doctoral degree = 13 (2.4%) Other = 4 (0.7%)	
Job Role	IT Professional = 295 (53.8%) End-user = 253 (46.2%)	
Work Experience (years)	14.69	11.25
IT Experience (years)	8.71	9.39

Measurement Model

Bootstrapping was employed to facilitate the evaluation significance of model path estimates. SmartPLS 3.3.2 was used for analyzing data (Ringle et al., 2015), employing bootstrapping with 5,000 re-samples following (Hair et al., 2017). The SmartPLS measurement model statistics include reliability, convergent validity, discriminant validity, and common method variance.

PLS analysis consists of two stages: (1) an assessment of the measurement model and (2) the assessment of the structural model.

Internal reliability was tested for measurement model assessment using factor loadings and composite reliability values. First, Cronbach's alpha was analyzed to estimate the reliability based on inter-correlations of the observed indicator variables. In addition, composite reliability was also considered to check different outer loadings of the indicators. Most of the latent variables and their indicators are good range between 0.7 and 0.9; however, the average variance extraction (AVE) of eustress is 0.461, below the threshold of 0.5 (Fornell & Larcker, 1981). Therefore, that required an evaluation of convergent validity since there were two items in the eustress with low outer loadings, including eust1 and eust4 with outer loadings of 0.077 and 0.130. Indicators with very low outer loading (below 0.4) were suggested to be eliminated from the latent variable (Bagozzi et al. 1991; Hair et al. 2011). Therefore, the two items were removed to improve the construct's convergent validity. The average variance extracted (AVE), which is equivalent to the communality of the construct, was also improved to 0.792 after the two items were removed. Table 4.2 contains the values supporting the conclusion of measurement instrument validity and reliability.

Table 4.2

Construct Reliability and Validity

Construct	Composite Reliability	Cronbach's Alpha	Average Variance Extracted (AVE)
Security techno-overload	0.955	0.940	0.808
Security techno-uncertainty	0.833	0.783	0.712
Security techno-complexity	0.932	0.908	0.845
SETA Availability	0.888	0.836	0.692
SETA Effectiveness	0.842	0.745	0.654
Security techno-reliability	0.881	0.842	0.671
Security Technical Support	0.903	0.862	0.782
Knowledge Sharing	0.893	0.820	0.735
Security Techno-Distress	0.960	0.948	0.842
Security Techno-Eustress	0.884	0.827	0.628
Security Carelessness	0.938	0.912	0.791
Resource Misuse	0.943	0.925	0.796
Security Procrastination	0.956	0.943	0.814

All the factor loadings of items on their associated latent variables are higher than 0.7 and were significant at $p < 0.001$; therefore, it suggests that the measurement model has strong convergent validity. In fitting the model, composite reliabilities (range from 0.842 to 0.956) confirm the internal reliability. Also, Cronbach's alpha (range from 0.745 to 0.948) suggests an internal consistency.

Discriminant validity was evaluated by comparing the square root of AVE to the correlations among the constructs, as shown in Table 4.3. All are higher than the correlations between the construct and the other variables, indicating that the measurement model has strong discriminant validity.

Table 4.3

Correlations Table

	1	2	3	4	5	6	7	8	9	10	11	12	13
1.Security techno-overload (STO)	0.89												
2.Security techno-uncertainty (STU)	0.34	0.84											
3.Security techno-complexity (STC)	0.69	0.21	0.92										
4.SETA Availability (SETA)	0.14	0.39	-0.01	0.83									
5.SETA Effectiveness (SETE)	0.08	0.38	-0.09	0.77	0.81								
6.Security techno-reliability (STR)	-0.07	0.29	-0.18	0.51	0.49	0.82							
7.Security technical support (TS)	0.03	0.33	-0.10	0.58	0.58	0.53	0.88						
8.Security knowledge sharing (KS)	0.18	0.31	0.05	0.54	0.57	0.48	0.50	0.86					
9.Security techno-distress (Dist.)	0.65	0.25	0.78	0.02	-0.02	-0.18	-0.06	0.06	0.92				
10.Security techno-eustress (Eust.)	0.57	0.30	0.41	0.36	0.33	0.19	0.25	0.32	0.46	0.79			
11.Security Carelessness (SC)	0.67	0.17	0.76	0.06	0.01	-0.16	-0.02	0.08	0.71	0.50	0.89		
12.Resource Misuse (RM)	0.51	0.08	0.65	-0.05	-0.05	-0.17	-0.03	-0.02	0.66	0.32	0.77	0.89	
13.Security Procrastination (SP)	0.58	0.09	0.68	-0.04	-0.06	-0.19	-0.06	0.01	0.68	0.41	0.82	0.79	0.90

Note: the diagonal values (bold) represent the square root of AVE

Furthermore, the cross-loadings among all measurement items were checked. Cross-loadings suggested indicators associated with construct should be greater than any of its cross-loadings on other constructs. The results of these two tests indicated that the measurement model has good discriminant and convergent validity, see Table 4.4.

Because of the dependent variable, counterproductive behaviors have a high correlation, including misuse, carelessness, and procrastination; therefore, we argue that these three constructs operationalize as a second-order construct with first-order reflective and second-order formative to form the information security counterproductive behaviors. The second-order constructs (security job demands, security job resources, and security counterproductive behaviors) measurement quality were evaluated by following the suggestions in previous studies and was directly measured using items from all the first-order constructs (Bock et al., 2005; Diamantopoulos & Winklhofer, 2001; Petter et al., 2007). Specifically, the repeated indicator approach (also known as the hierarchical component model) was applied based on the reflective-formative hierarchical component model testing results.

This approach measures the second-order factor using the observed latent variables for loading all the first-order factors (Ciavolino & Nitti, 2013; Hair et al., 2017). For formative second-order construct significance testing, job demands weights from the first-order constructs: techno-overload, techno-uncertainty, and techno-complexity to the second-order construct were 0.488, 0.197, and 0.512, respectively. The t-statistics were greater than 1.96 in the 95% confidence interval level.

Table 4.4

Cross Loading

	STO	STU	STC	SETA	SETE	STR	TS	KS	Dist.	Eust.	SC	RM	SP
STO1 ¹	0.943	0.411	0.687	0.158	0.113	-0.077	0.043	0.171	0.683	0.55	0.692	0.476	0.566
STO2 ¹	0.944	0.406	0.71	0.114	0.044	-0.103	-0.001	0.159	0.698	0.502	0.688	0.498	0.567
STO3 ¹	0.923	0.354	0.637	0.125	0.092	-0.037	0.049	0.162	0.625	0.516	0.61	0.433	0.509
STO4 ^{1*}	0.803	0.383	0.574	0.171	0.11	-0.026	0.077	0.193	0.588	0.464	0.523	0.459	0.466
STO5 ^{1*}	0.922	0.453	0.664	0.153	0.08	-0.076	0.047	0.155	0.681	0.535	0.645	0.553	0.55
STU1 ¹	0.454	0.885	0.188	0.334	0.356	0.276	0.298	0.306	0.217	0.286	0.132	0.052	0.061
STU2 ¹	0.460	0.737	0.163	0.273	0.288	0.333	0.291	0.268	0.123	0.157	0.037	0.008	-0.001
STU3 ¹	0.458	0.908	0.240	0.32	0.342	0.215	0.28	0.268	0.267	0.307	0.209	0.123	0.126
STU4 ^{1*}	0.419	0.705	0.245	0.437	0.432	0.438	0.439	0.332	-0.005	0.202	-0.014	-0.013	-0.061
STC1 ¹	0.671	0.22	0.916	0.013	-0.051	-0.139	-0.031	0.059	0.718	0.396	0.708	0.55	0.577
STC2 ¹	0.631	0.152	0.905	-0.04	-0.123	-0.173	-0.102	0.014	0.733	0.341	0.711	0.625	0.658
STC3 ¹	0.687	0.217	0.936	-0.017	-0.073	-0.178	-0.052	0.072	0.748	0.406	0.741	0.622	0.66
SETA1 ¹	0.207	0.383	0.065	0.908	0.676	0.428	0.548	0.537	0.075	0.402	0.133	0.017	0.02
SETA2 ¹	0.031	0.221	-0.051	0.742	0.499	0.4	0.383	0.332	0.004	0.214	0.000	-0.075	-0.047
SETA3 ¹	0.032	0.216	-0.052	0.702	0.505	0.4	0.388	0.332	0.022	0.215	-0.010	-0.035	-0.051
SETA4 ¹	0.042	0.27	-0.123	0.819	0.669	0.479	0.482	0.436	-0.087	0.218	-0.054	-0.141	-0.118
SETE1 ¹	0.14	0.362	-0.023	0.73	0.891	0.436	0.509	0.491	0.03	0.349	0.067	-0.039	-0.022
SETE2 ¹	-0.056	0.277	-0.197	0.499	0.751	0.418	0.376	0.368	-0.158	0.118	-0.118	-0.152	-0.18
SETE3 ¹	-0.061	0.271	-0.197	0.492	0.647	0.418	0.388	0.368	-0.154	0.103	-0.136	-0.147	-0.187
SETE4 ¹	0.043	0.31	-0.089	0.593	0.847	0.419	0.506	0.528	-0.033	0.261	0.001	-0.042	-0.068
STR1 ¹	-0.042	0.263	-0.114	0.443	0.414	0.855	0.437	0.404	-0.12	0.191	-0.087	-0.082	-0.127
STR2 ¹	-0.108	0.243	-0.192	0.391	0.417	0.802	0.45	0.406	-0.169	0.147	-0.159	-0.17	-0.181
STR3 ¹	-0.039	0.253	-0.136	0.432	0.407	0.819	0.422	0.389	-0.14	0.171	-0.119	-0.149	-0.146
STR4 ^{1*}	-0.085	0.248	-0.155	0.417	0.448	0.793	0.433	0.398	-0.135	0.119	-0.147	-0.125	-0.179
TS1 ¹	0.009	0.329	-0.094	0.547	0.571	0.497	0.866	0.456	-0.069	0.229	-0.022	-0.037	-0.069
TS2 ¹	-0.067	0.25	-0.214	0.472	0.482	0.532	0.698	0.384	-0.183	0.095	-0.165	-0.156	-0.196
TS3 ¹	0.063	0.282	-0.009	0.502	0.487	0.44	0.906	0.447	-0.005	0.275	0.048	0.006	0.002
TS4 ¹	0.003	0.294	-0.088	0.493	0.493	0.478	0.881	0.396	-0.041	0.209	-0.015	-0.016	-0.062
KS1 ¹	0.132	0.302	0.049	0.493	0.514	0.422	0.419	0.836	0.079	0.311	0.077	0.002	-0.015
KS2 ¹	0.164	0.289	0.046	0.478	0.504	0.394	0.408	0.877	0.065	0.358	0.077	0	0.047
KS3 ¹	0.152	0.257	0.04	0.427	0.471	0.44	0.439	0.858	0.011	0.299	0.033	-0.025	-0.022
Dist.1	0.668	0.252	0.732	-0.005	-0.011	-0.152	-0.032	0.053	0.927	0.457	0.652	0.645	0.682
Dist.2	0.642	0.224	0.705	0.018	-0.027	-0.186	-0.06	0.051	0.907	0.377	0.681	0.596	0.642
Dist.3	0.658	0.222	0.716	0.035	-0.039	-0.129	-0.021	0.066	0.918	0.454	0.695	0.602	0.648
Dist.4	0.665	0.225	0.735	0.04	-0.049	-0.13	-0.04	0.067	0.9	0.455	0.683	0.671	0.657
Dist.5	0.646	0.228	0.705	0.027	-0.031	-0.213	-0.081	0.051	0.88	0.391	0.698	0.664	0.649
Eust3	0.429	0.29	0.324	0.349	0.333	0.176	0.248	0.364	0.38	0.827	0.398	0.343	0.35
Eust5	0.568	0.266	0.415	0.304	0.242	0.157	0.19	0.317	0.523	0.915	0.493	0.437	0.431
Eust6	0.561	0.254	0.379	0.32	0.272	0.144	0.193	0.322	0.47	0.916	0.462	0.386	0.378
Eust7*	0.504	0.285	0.365	0.352	0.302	0.195	0.261	0.334	0.448	0.898	0.438	0.361	0.35
SC1 ¹	0.638	0.139	0.695	0.035	-0.011	-0.175	-0.02	0.034	0.684	0.444	0.904	0.715	0.772
SC2 ¹	0.648	0.115	0.689	0.038	-0.028	-0.156	-0.048	0.028	0.698	0.441	0.907	0.714	0.775
SC3 ¹	0.634	0.14	0.673	0.053	0.012	-0.12	0.024	0.069	0.662	0.458	0.892	0.711	0.777
SC4 ¹	0.623	0.212	0.645	0.09	0.092	-0.078	0.081	0.141	0.635	0.462	0.853	0.613	0.661
SC5 ¹	0.609	0.139	0.697	0.001	-0.079	-0.159	-0.044	0.05	0.683	0.427	0.886	0.736	0.786
SC6 ¹	0.560	0.120	0.685	0.009	-0.05	-0.164	-0.089	0.001	0.673	0.415	0.893	0.775	0.769
RM1 ¹	0.333	0.049	0.546	-0.081	-0.082	-0.157	-0.022	-0.023	0.526	0.261	0.636	0.797	0.671
RM2 ¹	0.346	0.048	0.478	-0.092	-0.073	-0.176	-0.011	-0.052	0.512	0.163	0.615	0.857	0.644
RM3 ¹	0.515	0.107	0.641	-0.026	-0.071	-0.132	-0.018	0.01	0.641	0.36	0.751	0.907	0.772
RM4 ¹	0.469	0.07	0.615	-0.043	-0.045	-0.122	-0.013	0.01	0.634	0.313	0.706	0.921	0.719
RM5 ¹	0.65	0.196	0.709	0.086	0.001	-0.119	0.013	0.109	0.685	0.495	0.798	0.893	0.801
SP1 ^{1*}	0.56	0.127	0.654	0.025	-0.045	-0.101	0.001	0.058	0.663	0.415	0.794	0.705	0.913
SP2 ¹	0.509	0.055	0.608	-0.051	-0.078	-0.199	-0.054	-0.025	0.642	0.385	0.769	0.738	0.939
SP3 ¹	0.553	0.06	0.634	-0.083	-0.089	-0.223	-0.071	-0.016	0.681	0.366	0.768	0.771	0.921
SP4 ¹	0.575	0.131	0.664	0.037	-0.053	-0.101	-0.02	0.058	0.683	0.417	0.802	0.765	0.883
SP5 ¹	0.482	0.071	0.606	-0.051	-0.119	-0.134	-0.088	-0.037	0.639	0.349	0.778	0.800	0.866

Table 4.4 Notes:

STO = Security techno-overload; STU = Security techno-uncertainty; STC = Security techno-complexity; SETA = SETA Availability; SETE = SETA Effectiveness; STR = Security techno-reliability; TS = Security technical Support; KS: Security knowledge sharing; Dist. = Distress; Eust. = Eustress; SC = Carelessness; RM = Resource Misuse; SP = Security Procrastination

* = *new items*

Item¹ = first-order latent variables

Second-order latent variables: security job demands comprised of STO, STU, and STC, security job resources comprise of SETA, SETE, STR, TS, and KS.

Security counterproductive behavior comprises of SC, RM, and SP.

Regarding to security job resources, the weights from security awareness training availability (SETA), security awareness training effectiveness (SETE), security techno-reliability, technical support, and knowledge sharing were 0.307, 0.224, 0.256, 0.248, and 0.186, respectively, and the t-statistics were greater than 2.58, which met the formative construct specifications. Also, the path coefficient to counterproductive behaviors from first-order constructs: security carelessness, information systems resource misuse, and security procrastination were 0.389, 0.341, 0.316 with t-statistics much larger than the threshold t-value of 1.96.

Variance inflation factor (VIF) tests were performed to determine if multicollinearity issues among the first-order constructs exist. The results show that the VIF values of techno-overload, techno-uncertainty, and techno-complexity on the second-order construct of security job demand were below the cutoff of 5 (2.343, 1.139, 2.156, respectively). VIF values of SETA, SETE, security techno-reliability, technical support, and knowledge sharing on the job resources were also below the threshold of 5 (2.781, 2.873, 1.855, 1.988, and 1.619). VIF values of security carelessness, information systems resource misuse and security procrastination on the counterproductive behaviors were (4.625, 4.768, and 4.028) (Lee et al., 2018; Hair et al., 2013).

As a result, there are no concerns regarding problematic multicollinearity association with the first-order components of security job demand, security job

resource, and security counterproductive behavior (Hair et al., 2013; Petter et al., 2007).

Common Method Variance

Common method bias is problematic in the study since data collection is collected at one point in time, which refers to the amount of spurious covariance shared among variables because of the common method used in data collection (Podsakoff et al., 2003). The problem often exists in studies that use the survey method when respondents take a single survey at the same point in time.

Several preventative steps recommended by (Podsakoff et al., 2003) were used to mitigate the common method variance. These included steps including protecting respondent anonymity, adding open text for participants' position and occupation and years of work experience and months in current position, and improving scale measurements with different scale points and formats (7 Likert-scale "Strong disagree" to "Strong agree," bipolar scale) and marker variable (unrelated theoretical construct, "blue attitude") was used to report in the result that the steps work since there is not CMV.

First, Harman's single factor test was conducted. CMV is concerned if the factor analysis results in a single factor or if one general factor accounts for more than 50% of the covariance. Based on the result of this factor analysis, the single largest eigenvalue factor accounts for 33.88% of the variance, suggesting that the majority of variance is not accounted for by just one single general factor and indicates that problematic common method variance is unlikely.

Second, a marker variable analysis was employed using a three-item scale for "blue attitude," which is theoretically unrelated to the other main variables. Then, a model was constructed with the added marker variable to the endogenous variable to

assess the common method bias (Lindell & Whitney, 2001; Tehseen et al., 2017). If the mean correlation among all latent variables and the marker variable is more than 0.3, this indicates there is a common method bias issue (Tehseen et al., 2017). After examining the mean correlation among all the variables and marker variables, the result is 0.163, much less than the 0.3 thresholds (Tehseen et al., 2017). Therefore, it suggests no evidence of problematic common method bias in this study.

Structural Model

The structural model was deployed in SmartPLS to evaluate the significance and strength of each of the hypothesized effects. The research model provided greater predictive efficacy for security techno-distress ($R^2 = 64.8\%$) than eustress ($R^2 = 39.1\%$), and the R^2 for counterproductive behaviors is 67.9%. R^2 values reflect the amount of variance explained by the model or the model's predictive power, are presented within the oval of each endogenous variable. In this study, the model accounted for more of the variance in distress than eustress. Distress and eustress, together, account for a moderate amount of the variance in counterproductive behaviors.

Table 4.5 presents results related to the hypotheses derived from the research model. Results indicate overall support for the model, with five of six hypotheses supported ($p < 0.001$). The relationship between security job demands and distress was significant ($\beta = 0.825$, $p < 0.001$), lending support to H1a. Job resources was negatively associated with distress ($\beta = -0.133$, $p < 0.001$) while security job resources was positively associated with eustress ($\beta = 0.318$, $p < 0.001$), that supported the H2a and H2b. Furthermore, distress toward the security counterproductive behaviors was positively associated ($\beta = 0.594$, $p < 0.001$).

Table 4.5

Results

Hypotheses/Path	Path Coefficient	t-statistics	p-value	Support	Effect size (f^2)	Effect size interpret
H1a: Security Job demands->security-techno distress	0.825	47.138	<0.001	Yes	1.162	Large
H1b: Security Job demands->security-techno eustress	0.529	16.295	<0.001	No*	0.330	Large
H2a: Security Job resources->security-techno distress	-0.133	5.063	<0.001	Yes	0.035	Small
H2b: Security Job resources->security-techno eustress	0.318	8.480	<0.001	Yes	0.073	Medium
H3: Security-techno distress->Security Counterproductive Behaviors	0.594	15.973	<0.001	Yes	0.717	Large
H4: Security-techno eustress->Security Counterproductive Behaviors	0.045	1.780	0.077	No	0.009	Negligible

* - H1b indicated a negative relationship, so H1b is not supported.

Therefore, the H3 was supported. Moreover, report the f^2 - Cohen et al. (2003) Largest effect of distress 0.35. Guidelines for assessing f^2 are that values of 0.02, 0.15, and 0.35, respectively, represent small, medium, and large effects (Cohen, 1988) of the exogenous latent variable.

R^2 values of all endogenous constructs, the change in the R^2 value when a specified exogenous construct is omitted from the model can be used to evaluate whether the omitted construct has a substantive impact on the endogenous constructs. This measure is the f^2 effect size (Hair et al., 2017).

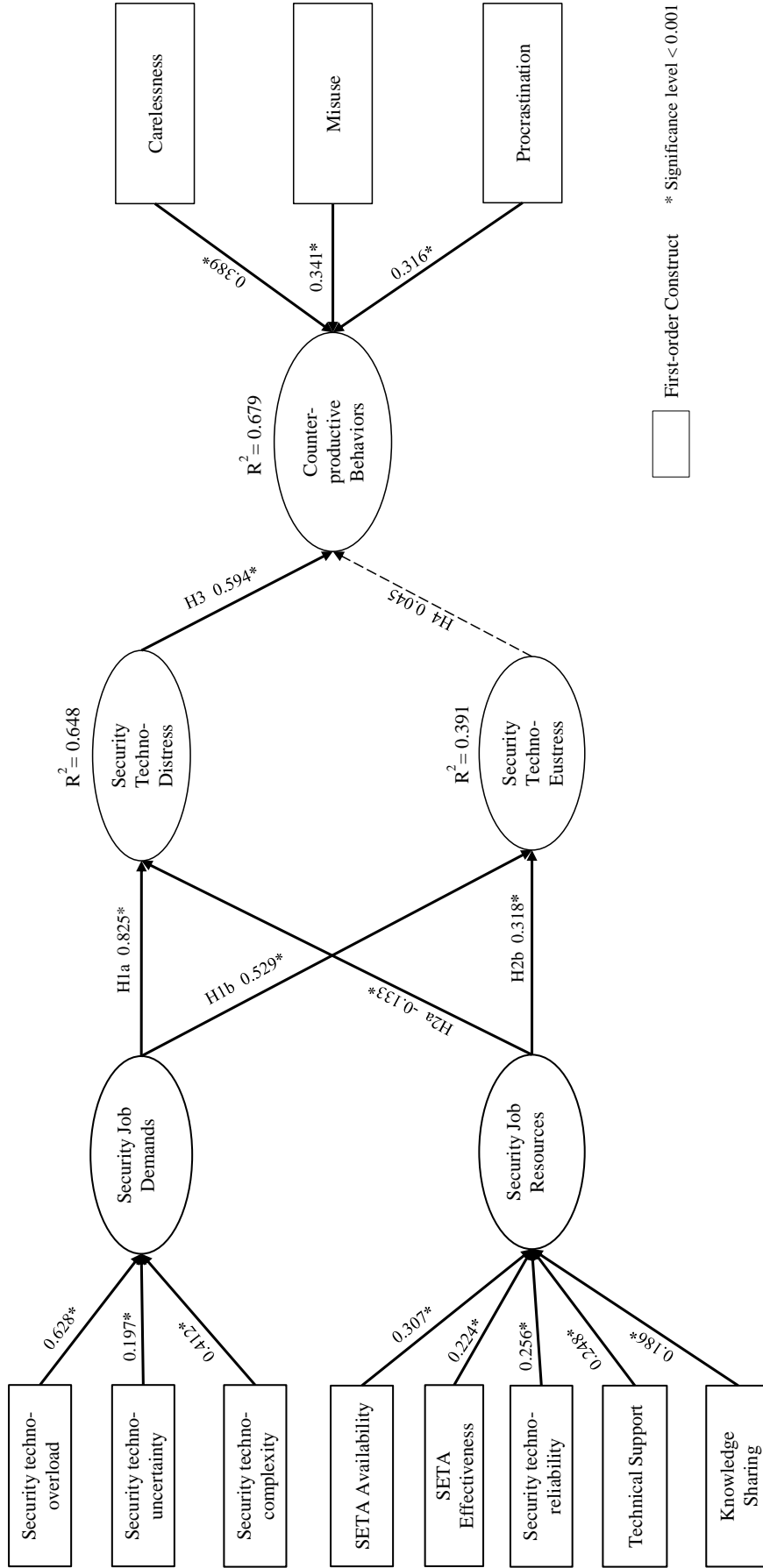
The hypotheses H1b and H4 (security job demands to eustress and security-techno eustress to counterproductive behaviors) were not supported. H1b was

opposite to the hypothesis ($\beta = 0.529, p < 0.001$), and H4 was not significant ($\beta = 0.045, p = 0.077$). The results of path model significance were represented graphically in Figure 4.1.

It was also noted that the relationships on the endogenous variable (counterproductive behaviors) with the control variables education, gender (dummy variable male = 0, and female = 1), and self-efficacy were not statistically significant. However, job role (dummy variable with IT = 0, non-IT = 1) had a statistically significant negative relationship with security counterproductive behaviors ($\beta = -0.218, p < 0.001$) and age had a statistically significant negative relationship with security counterproductive behavior ($\beta = -0.162, p < 0.001$).

Table 4.6 shows the total effects of security job demand and resource factors on information security counterproductive behaviors. Based on the results, security techno-distress shows the strongest effect on counterproductive behavior outcomes (total effect = 0.777). Besides, security job demand factors have stronger effects on information security counterproductive behaviors outcomes than resource factors. Security techno-overload (total effect = 0.245), security techno-complexity (total effect = 0.471), while security techno-uncertainty has insignificant effect (total effect = 0.023).

Most of the security job resource factors do not significantly affect information security counterproductive behavior outcomes except the security techno-reliability (total effect = -0.065) and SETA (total effect = -0.073).



Notes: * - Path $p < 0.001$; Path in dash is not significant ($p > 0.05$).

Figure 4.1: Model Result

Table 4.6

Total Effects of Antecedent Variables on Security Counterproductive Behaviors

	Effect Size	t-stat	p-value
Security techno-Overload -> CPB	0.245	12.501	<0.001
Security techno-Uncertainty -> CPB	0.023	0.867	0.386
Security techno-Complexity -> CPB	0.471	12.501	<0.001
SETA Availability -> CPB	-0.073	2.232	0.026
SETA Effectiveness -> CPB	-0.032	0.907	0.365
Security techno-Reliability -> CPB	-0.065	2.21	0.027
Security Technical Support -> CPB	-0.004	0.126	0.900
Security Knowledge Sharing -> CPB	-0.013	0.517	0.605
Security techno-Distress -> CPB	0.777	28.711	<0.001
Security techno-Eustress -> CPB	0.056	0.934	0.077
Education -> CPB	-0.005	0.130	0.897
Gender -> CPB	0.063	1.931	0.051
Age -> CPB	-0.162	4.044	<0.001
Job role -> CPB	-0.218	6.731	<0.001
Self-efficacy -> CPB	-0.035	1.080	0.792

Note: CPB – Security Counterproductive Behaviors

CHAPTER 5

DISCUSSION AND CONCLUSIONS

This study aimed to examine the information security technostress creators (hindrance stressors) and stress inhibitors (challenge stressors) on negative and positive stress responses that eventually impact the counterproductive security behaviors. The first message from this study is that the individual perception is important; it is not whether dealing with information security technology is complex but whether employees see it as complex or not. Therefore, it is important to simplify the information security complexity to reduce employees' perceptions of complexity, reducing their negative stress responses and strengthening their positive stress responses.

Overall, this study's findings indicate support for the research model, with four out of six hypotheses supported (H1a, H2a, H2b, and H3), at the significant level $p < 0.001$. The path corresponding to H1b was significant but indicated a positive relationship while hypothesizing a negative relationship. The findings indicate that distress by far has the most positive significant effect on counterproductive behavior outcomes. Also, total effects suggest that two factors among three security job demand factors, security techno-overload (total effect = 0.245) and security techno-complexity (total effect = 0.471), strongly affect security counterproductive behavior. These results imply that reducing perceptions of information security technology complexity is

useful for reducing counterproductive security behaviors. Reducing security technology overload perceptions should also be useful.

On the other hand, the findings related to the effects of security job resource factors on counterproductive behavior suggest that security techno-reliability (total effect = -0.065) and SETA (total effect = -0.073) have significant effects on counterproductive behaviors, which suggest that security techno-reliability may reduce the security distress (bad stress) impacts of information security technology. The finding is consistent with previous studies that suggest techno-reliability helps reduce individual strain (Ayaagari et al., 2011), which implies in the information security technology context that if these features and characteristics are reliable in their performance, then employees' experience is not stressful. Information security professionals should also consider emphasizing security technology reliability and explaining how these features are important and helpful in protecting employees' and organizations' digital assets. While the importance of security training and awareness and availability (SETA) have been emphasized in InfoSec literature (D'Arcy et al., 2009; D'Arcy et al., 2014; Herath & Rao, 2009; Posey et al., 2014; Yoo et al., 2019), the results of this study indicate that only SETA awareness has a significant effect on counterproductive behaviors; perceptions of SETA effectiveness did not have a significant on counterproductive behaviors.

This study demonstrated that assisting and training employees could effectively increase security techno-eustress since they may enhance the positive challenge stress response and mitigate the negative stress response that eventually impacts employees' tendency of counterproductive behaviors. Specifically, this study emphasized and examined the two antecedents (security job demands and security job resources) that

positively influence positive stress response (security-techno eustress) while the security job demands positively affects negative stress response (security-techno distress) and job resources negatively influence the distress. More interestingly, the findings show that job resources including information security reliability, security awareness training availability, security awareness training effectiveness, technical support, and knowledge sharing are all helpful in mitigating the distress, and also have a significant positive relationship on eustress suggesting that these factors encourage employees to prepare well for challenges interacting with information security technology. This is consistent with previous studies that recommended the SETA and technical support (Sykes, 2015; Herath & Rao, 2009a; Herath & Rao, 2009b; Puhakainen & Siponen, 2010; Ragu-Nathan et al., 2008).

The hypothesized negative relationship between job demands and eustress was not supported since the security job demands had a significant positive effect on eustress. A plausible explanation for the positive relationship between the security job demands and eustress may be that those demands create the condition for eustress to exist because there is no need to cope unless there is demand. If there is no demand or low demand, there is no challenge; that is necessary eustress to be present. If there is no demand, there is no need to find and experiment with a new way to complete tasks. Future research should examine this relationship further (Hargrove et al., 2015).

Counterproductive behaviors (security procrastination, information systems resource misuse, and security carelessness) are highly correlated because there is a positive likelihood of employees committing to one behavior; the other two behaviors may follow. The positively significant relationship between distress and

counterproductive behaviors indicates that the stronger bad stress employees experience caused by demands rooted in information security technology, the higher the chance that they may engage in information security counterproductive behaviors. This finding is consistent with (D'Arcy et al., 2014; Hwang & Cha, 2018), who found that overwhelming stress on employees may increase incidents by insider actors.

The model is more effective at accounting for the variance in distress than eustress. The relationship between eustress and counterproductive behaviors is insignificant, so this study's findings do not support previous studies that examined the eustress, which suggested that eustress is good stress that helps mitigate negative psychological outcomes (Califf et al., 2020; Hargrove et al., 2013; Simmons & Nelson, 2007). One plausible explanation for this result is that there is no motivation from the employees' positive stress response that makes them avoid counterproductive security behaviors since employees may often prioritize achieving work goals over security. Previous InfoSec studies suggested that employees are often pragmatic and care about their job performance more than they care about information security. It is important to evaluate employees' performance not based on just business needs but also on information security awareness as well (D'Arcy et al., 2014; Guo et al., 2011).

This study followed Chu and Chau (2014)'s future research calls for research that examines the effect of individual factors such as age that may influence employees' probabilities of committing resource misuse or security careless. The study's findings show that job role and age have significantly negative relationships with distress and counterproductive behaviors, which suggest that the older the employees become, the less likely they will engage in counterproductive behaviors. Also, because older colleagues

are risk-averse, they tend to have higher concerns and experience more distress than younger colleagues regarding information security practice. Also, a plausible explanation for the job role is consistent with the previous study that suggests non-IT employees often deal with less demand than IT employees because IT employees have to deal with all the technical and managerial security factors (Lee et al., 2016).

Theoretical Contributions

First, this study contributes to research by shedding light on the inter-correlations of three specified security counterproductive behaviors: security carelessness, information systems resource misuse, and security procrastination. The lack of empirical studies on security counterproductive behaviors encourages the study of what demand and resource factors may cause and minimize the counterproductive behaviors in information security discipline, which answer the call for future research (Chu & Chau, 2014; Ifinedo, 2019). Also, some third variables might influence security counterproductive behavior as correlation can be because of a causal relationship. However, more likely, this case is that there might be a third variable that affects all of these.

Second, security carelessness, security procrastination, and information systems resource misuse share similar effects on counterproductive behaviors. This study examines the robustness of the JD-R model with a negative behavioral outcome related to the information security context. A counterproductive behavior has been conceptualized and treated as a multidimensional construct in management and psychology disciplines (Fox & Spector, 2005; Fox & Spector, 2001; Sackett, 2002; Dilert et al., 2007). The InfoSec literature focuses on information security policy compliance intention, which

does not sufficiently account for an intention-behavior gap and largely ignores other types of information security behaviors (Cram et al., 2019). This study attempted to bring attention to the three counterproductive information security behaviors to understand further employees' behaviors interacting with information security technology.

Third, this study integrates JD-R and technostress-trifecta to examine and identify relevant security demand and resource factors that may impact security distress (detrimental stress) and eustress (beneficial stress) and the total effect of these two types of stress responses (negative and positive stress response) toward security counterproductive behavior outcome. Each has different concepts and relationships among these two constructs (Tarafdar et al., 2017).

Finally, this study looked at security-related stress, mainly focusing on the information security technology aspect, which has not been examined previously. This study also further includes the security demands and security resources from the JD-R framework. While previous security-related technostress mainly focused on negative aspects (D'Arcy et al., 2014; Hwang & Cha, 2018; Hwang & Cha, 2021), information system resources organizations often have to tackle or mitigate security threats, and was the positive stress response were ignored. This study's findings suggest that security job demands and security job resources explain a large portion of distress, but smaller yet still highly significant of eustress variance. More importantly, CPB is all about distress, and eustress does not make any difference.

Practical Contributions

Security job demands and resources explain the large portion of the variance in distress but a smaller but still highly significant portion of the variance in techno-eustress.

These findings imply that organizations should provide sufficient resources related to security and should also consider intervention programs to reduce distress related to using security technologies. Also, the effect of distress on counterproductive behaviors indicates that organizations may find it useful to understand better how to help employees deal with ever-changing and complex information security technologies. When firms invest in more new information security technology, these new technologies require employees to put more effort into completing work-related tasks, which may cause distress. Also, using these technologies may consume a large amount of employees' time due to the need to update knowledge and gather necessary skills to deal with the upgrades on new information security technology. As a result, employees will find a way to engage in security counterproductive behavior when they are expected to get work-related tasks done. Therefore, management needs to care about employees' security techno-distress. Management and information technology departments may also need to be mindful of seeking solutions to minimize employees' information security counterproductive behaviors; they should clearly emphasize which are dangerous and may make employees and organizations vulnerable to cyber threats. At the same time, it is important to provide more simplified explanations about security procedures to reduce complexity and think about a balanced strategy to mitigate security techno-overload. Also, it is important to align security objectives and employees' goals. IT and Management departments need to pay careful attention to balancing security needs such as automatic updates and password change frequency with the need to efficiently complete work tasks. Otherwise, employees may act in counterproductive ways to the organization's security goals.

Counterproductive behavior has only effect from techno-distress but not from techno-eustress. Distress shows the largest effect from the findings; therefore, it is suggested that organizations may consider designing a meditation or stress relief or mindfulness training for employees to reduce negative stress experiences.

The findings give managers a clearer picture of how some forms of information security counterproductive behaviors, security carelessness, information systems resource misuse, and security procrastination could be interrelated. That means once employees engage in one of the security counterproductive behaviors, they are more likely to engage in the other two. The three instruments may help design decision support systems and provide knowledge in developing systems for security decision-making and planning in organizations. Practitioners need to proactively strengthen security education and training awareness to emphasize the dangers of counterproductive behaviors across different information technology devices that employees use for their work tasks. Security awareness training needs to emphasize all three activities, including encouraging the good security routine of updating passwords, carefully considering appropriate information systems resource use such as double-checking software sources, and constantly logging out of systems after use. Also, managers may try to frame SETA and find a technological solution to reduce security complexity and workload. This study provides organizations with measures to consider managing employees' technostress and stress response experienced from information security technology as an important strategy to improve information security and mitigate security incidents incurred by insider actors. Hopefully, the findings encourage managers to have older employees train and advise younger colleagues and design culture of knowledge sharing and raise more

awareness toward the younger employees who are more risk-taking and often more likely to participate in security counterproductive behaviors.

Limitations and Future Research

While the study was developed and based on a reasonable theoretical framework and was tested with a reliable survey instrument, limitations were still present that could be addressed in future research. First, the study examined only one behavioral outcome, while psychological outcomes were not considered. Second, this study used a cross-sectional approach by collecting data at a single point in time, limiting the ability to make definitive claims regarding causality. As with any empirical study relying on self-reported data, the results could be subject to response and social desirability biases. Third, there might often be a possibility of inherent social desirability bias from the self-report process from respondents. Fourth, although there was unlikely multicollinearity among the first-order constructs on the formative second-order constructs of security job demand, security job resource, and the counterproductive behaviors, the first-order constructs on the counterproductive behaviors may need to be further evaluated in the future study due to close VIFs value to the threshold of 5.

Psychological and behavioral outcomes are associated with the job demand-resources framework (Bakker & Demerouti, 2017). This study looked at the only behavioral outcome, which is the counterproductive behaviors (carelessness, misuse, and procrastination); therefore, future research is encouraged to explore further the psychological and well-being outcomes such as exhaustion, job satisfaction, psychological contract fulfillment, to understand further the causal effects of resources and demands employee-information security technology interaction that influence on

employee's outcomes. In addition, more recent JD-R suggests the concept of personal resources (i.e., optimism, self-esteem, resilience), which refers to beliefs about how much control an individual has over their environment (Bakker & Demerouti, 2014; Bakker & Demerouti, 2017). This study did not include personal resources, and future studies are encouraged to examine and investigate them.

Changes over time represent an important factor not considered in this study. Future research may examine the changing effects in security distress and security eustress. For future research, the longitudinal approach could be helpful to gain a better understanding of causality when examining the relationship between these constructs in different points in time.

Furthermore, Lazarus and Launier (1978) view stress as a process involving a transaction between the individual and the environment appraisal process and coping process. Problem-focused coping, such as task or technology experimentation, may be associated with eustress that mediates the effect of eustress on outcomes. On the other side, avoidance coping associated with distress, such as withdrawal or venting, may affect the security behavioral outcomes.

As with any empirical study relying on self-reported data, the results are subject to response and social desirability biases. We attempted to counter these effects by carefully designing the questionnaire and ensuring anonymity and confidentiality. Moreover, we applied statistical techniques to identify dishonest reporting (e.g., we included control items to check if participants carefully read the instructions) and checked the validity and reliability of our results. Nevertheless, future work can further explore the effects using different experimental or mixed methods methodologies.

Finally, future research may design experimental studies that look at different approaches with two- or three levels at security techno-complexity and security techno-overload to further understand and strengthen the internal validity to demonstrate a causal relationship between security techno-complexity and overload with security counterproductive behaviors. In addition, two potential variables, including the level of complexity and novelty, could be manipulated through the experimental scenarios with high and low. Two-by-two experimental studies would also be helpful to consider nature of task(s) that future study may look at specific tasks and the degree of routine & non-routine since cognitive may be lower when employees do routine tasks. Furthermore, future research could design scenario-based and experiment studies based on the findings to leverage more important situational details in operationally characterizing the decision-making leading to the violation (Klepper & Nagin, 1989). Because the scenario-based approach provides a hypothetical other and their behavior in purely scenario-based terms, respondents will be less likely to conceal their intentions and reactions in response to the manipulation (Trevino, 1992).

REFERENCES

- AIS. (2019). 42 Worrying workplace stress statistics. *The American Institute of Stress*. Retrieved from <https://www.stress.org/42-worrying-workplace-stress-statistics>.
- Ahuja, M., Chudoba, K., Kacmar, C., McKnight, D., & George, J. (2007). IT road warriors: Balancing work-family conflict, job autonomy, and work overload to mitigate turnover intentions. *MIS Quarterly*, 1-17.
- Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS Quarterly*, 35(4), 831-858.
- Bagozzi, R., Yi, Y., & Phillips, L. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly*, 421-458.
- Bakker, A. B., & Demerouti, E. (2007). The job demands-resources model: State of the art. *Journal of Managerial Psychology*.
- Bakker, A., & Demerouti, E. (2017). Job demands–resources theory: Taking stock and looking forward. *Journal of Occupational Health Psychology* 22(3), 273.
- Bakker, A., Demerouti, E., De Boer, E., & Schaufeli, W. (2003). Job demands and job resources as predictors of absence duration and frequency, *Journal of Vocational Behavior*, 62(2), 341-356.
- Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, 689-710.
- Berinsky, A., Huber, G., & Lenz, G. (2012). Evaluating online labor markets for experimental research: Amazon. com’s mechanical turk. *Political Analysis*, 20(3), 351-368.
- Brod, C. (1984). *Technostress: The human cost of the computer revolution*. Addison-Wesley.
- Bock, G., Zmud, R., Kim, Y., & Lee, J. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological factors, and organizational climate. *MIS Quarterly*, 29(1), 87-111.

- Boss, S., Galletta, D., Lowry, P., Moody, G., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 523-548.
- Califf, C., Sarker, S., & Sarker, S. (2020). The bright and dark sides of technostress: A mixed-methods study involving healthcare IT. *MIS Quarterly*, 44(2).
- Cavanaugh, M., Boswell, W., Roehling, M., & Boudreau, J. (2000). An empirical examination of self-reported work stress among us managers, *Journal of Applied Psychology*. 85(1), 65.
- Cavusoglu, H., Cavusoglu, H., Son, J., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management* 52(4), 385-400.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, 16(1), 28-46.
- Chin, W. (1998). Commentary: Issues and opinion on structural equation modeling. *JSTOR*.
- Chu, A., & Chau, P. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems* (66), 93-101.
- Ciavolino, E., & Nitti, M. (2013). Using the hybrid two-step estimation approach for the identification of second-order latent variable models. *Journal of Applied Statistics* 40(3), 508-526.
- Cohen, S., Kamarck, T., & Mermelstein, R. (1983). A global measure of perceived stress. *Journal of Health and Social Behavior*, 385-396.
- Cooper, C., Dewe, P., & O'Driscoll, M. (2001). *Organizational stress: A review and critique of theory, research, and applications*. SAGE.
- Cooper, C., & Dewe, P. (2008). *Stress: A brief history*. Oxford.
- Cram, W., D'Arcy, J., & Proudfoot, J. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2).

- Crawford, E., LePine, J., & Rich, B. (2010). Linking job demands and resources to employee engagement and burnout: A theoretical extension and meta-analytic test. *Journal of Applied Psychology*, *95*(5), 834.
- Crossler, R., Andoh-Baidoo, F., & Menard, P. (2019). Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of US and Ghana. *Information & Management* *56*(5), 754-766.
- 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., Herath, T., & Shoss, M. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318.
- D'Arcy, J., Herath, T., Yim, M., Nam, K., & Rao, H. (2018). Employee moral disengagement in response to stressful information security requirements: a methodological replication of a coping-based model, *AIS Transactions on Replication Research*, *4*, 8.
- D'Arcy, J., & Hovav, A. (2009). Does One Size Fit All? Examining the Differential Effects of Is Security Countermeasures. *Journal of Business Ethics*, *89*(1), 59.
- D'Arcy, J., & Lowry, P. (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., & Teh, P. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*. *56*(7), 103-151.
- Dell. (2017). Dell end-user security survey. Accessed February 9, 2018, https://dell.com/sites/csdocuments/Learn_Docs/en/dell-end-user-security-survey-2017.pdf.
- DeLone, W., & McLean, E. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research*, *3*(1), 60-95.
- DeLone, W., & McLean, E. (2003). The delone and mclean model of information systems success: A ten-year update. *Journal of Management Information Systems* *19*(4), 9-30.
- Demerouti, E., Bakker, A., Nachreiner, F., & Schaufeli, W. (2001). The job demands resources model of burnout. *Journal of Applied Psychology*, *86*(3), 499.

- Demerouti, E., & Bakker, A. B. (2011). The job demands-resources model: Challenges for future research. *SA Journal of Industrial Psychology*, 37(2), 01-09.
- Diamantopoulos, A., & Winklhofer, H. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research*, 38(2), 269-277.
- Edwards, J., & Cooper, C. (1988). The impacts of positive psychological states on physical health: A review and theoretical framework. *Social Science & Medicine*, 27(12), 1447-1459.
- Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50.
- Fox, S., & Spector, P. (Eds.). (2005). *Counterproductive work behavior*. American Psychological Association.
- Fox, S., Spector, P., & Miles, D. (2001). Counterproductive work behavior (CWB) in response to job stressors and organizational justice: Some mediator and moderator tests for autonomy and emotions. *Journal of Vocational Behavior*, 59, 291–309.
- Fox, S., & Spector, P. (1999). A model of work frustration–aggression. *Journal of Organizational Behavior*, 20(6), 915-931.
- Fox, S., Spector, P., Goh, A., Bruursema, K., & Kessler, S. (2012). The deviant citizen: Measuring potential positive relations between counterproductive work behaviour and organizational citizenship behaviour. *Journal of Occupational and Organizational Psychology*, 85(1), 199-220.
- Galluch, P., Grover, V., & Thatcher, J. (2015). Interrupting the workplace: Examining stressors in an information technology context, *Journal of the Association for Information Systems* 16(1), 2.
- Gefen, D., Rigdon, E., & Straub, D. (2011). Editor's comments: An update and extension to sem guidelines for administrative and social science research. *MIS Quarterly*, iii-xiv.
- Gefen, D., Straub, D., & Boudreau, M. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, 4(1), 7.
- Guo, K., Yuan, Y., Archer, N., & Connelly, C. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems* 28(2), 203-236.

- Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2013). *A Primer on Partial Least Squares Structural Equation Modeling (Pls-Sem)*. SAGE.
- Hair, J., Ringle, C., & Sarstedt, M. (2011). Pls-Sem: Indeed a silver bullet. *Journal of Marketing theory and Practice* 19(2), 139-152.
- Hair Jr, J., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research, *European Business Review*.
- Hair, J., Sarstedt, M., Ringle, C., & Gudergan, S. (2017). *Advanced issues in partial least squares structural equation modeli*. SAGE.
- Hargrove, M., Becker, W., & Hargrove, D. (2015). The hrd eustress model: Generating positive stress with challenging work. *Human Resource Development Review* 14(3), 279-298.
- Hargrove, M., Nelson, D., & Cooper, C. (2013). Generating eustress by challenging employees: Helping people savor their work. *Organizational Dynamics*, 42, 61-69.
- Helkala, K., Knox, B., Jøsok, Ø., & Knox, S. (2016). Factors to affect improvement in cyber officer performance. *Information & Computer Security*.
- Herath, T., & Rao, H. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, *Decision Support Systems*, 47(2), 154-165.
- Herath, T., & Rao, H. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems* 18(2), 106-125.
- Hofstede, G. (2011). Dimensionalizing cultures: The hofstede model in context. *Online Readings in Psychology and Culture*, 2(1), 8.
- Hollinger, R. (1986). Acts against the workplace: Social bonding and employee deviance. *Deviant Behavior*, 7(1), 53-75.
- 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.
- Hwang, I., Kim, D., Kim, T., & Kim, S. (2016). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*. 41(1), 2-18.

- Hwang, I., Kim, S., & Rebman, C. (2021). Impact of regulatory focus on security technostress and organizational outcomes: The moderating effect of security technostress inhibitors. *Information Technology & People*.
- Ifinedo, P. (2019). End user nonmalicious, counterproductive computer security behaviors: Concept, development, and validation of an instrument. *Security and Privacy*, 2(3).
- Jiang, J., Klein, G., & Carr, C. (2002). Measuring information system service quality: Servqual from the other side, *MIS Quarterly*, 145-166.
- Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 549-566.
- 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.
- Kaspersky. (2019). *Report: The state of cyber-stress*. Retrieved from <https://Media.Kaspersky.Com/En/State-of-Cyber-Stress-Survey-Report.Pdf>.
- Kim, J., Park, E., & Baskerville, R. (2016). A model of emotion and computer abuse. *Information & Management*, 53(1), 91-108.
- Kirlappos, I., Beutement, A., & Sasse, M. (2013). Comply or die is dead: Long live security-aware principal agents. *International Conference on Financial Cryptography and Data Security*, Springer.
- Kirsch, L., & Boss, S. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. *ICIS 2007 Proceedings*, 103.
- Klepper, S., & Nagin, D. (1989). The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology*, 27(4), 721-746.
- Lazarus, R. (1995). Vexing research problems inherent in cognitive-mediational theories of emotion-and some solutions. *Psychological Inquiry*, 6(3), 183-196.
- Lazarus, R., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer.
- Lazarus, R., & Launier, R. (1978). Stress-related transactions between person and vironment. *Perspectives in Interactional Psychology*. Springer.
- LePine, J., LePine, M., & Jackson, C. (2004). Challenge and hindrance stress: relationships with exhaustion, motivation to learn, and learning performance. *Journal of Applied Psychology*, 8(95), 883.

- LePine, J., Podsakoff, N., & LePine, M. (2005). A meta-analytic test of the challenge stressor–hindrance stressor framework: An explanation for inconsistent relationships among stressors and performance. *Academy of Management Journal*, 48(5), 764-775.
- Lee, C., Lee, C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, 59, 60-70.
- Lee, J., de Guzman, M., Talebi, N., Korní, S., Szumigala, D., & Rao, H. (2018). Use of online information and suitability of target in shoplifting: a routine activity based analysis. *Decision Support Systems*, 110, 1-10.
- Li, Y., Yazdanmehr, A., Wang, J., & Rao, H. (2019). Responding to identity theft: A victimization perspective. *Decision Support Systems*, 121, 13-24.
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems* 11(7), 394-413.
- Lindell, M., & Whitney, D. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86(1), 114.
- Lowry, P., D'Arcy, J., Hammer, B., & Moody, G. (2016). Cargo cult science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including mechanical turk and online panels. *The Journal of Strategic Information Systems*, 25(3), 232-240.
- Lowry, P., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (Sem) for building and testing behavioral causal theory: when to choose it and how to use IT. *IEEE Transactions on Professional Communication*, 123-146.
- Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32-44.
- Marcoulides, G., & Chin, W. (2013). You write, but others read: Common methodological misunderstandings in pls and related methods. *New Perspectives in Partial Least Squares and Related Methods*. Springer.
- Merkow, M., & Breithaupt, J. (2014). Information security: Principles and practices. *Pearson Education*.

- Moore, S. (2020). Security and risk management spending growth to slow but remain positive in 2020. Retrived from <https://www.gartner.com/en/Newsroom/Press-Releases/2020-06-17-Gartner-Forecasts-Worldwide-Security-and-Risk-Management>.
- Nelson, D., & Cooper, C. (2007). *Positive Organizational Behavior*. SAGE.
- Neuman, J., & Baron, R. (1998). Workplace violence and workplace aggression: Evidence concerning specific forms, potential causes, and preferred targets. *Journal of Management*, 24(3), 391-419.
- O’Sullivan, G. (2011). The relationship between hope, eustress, self-efficacy, and life satisfaction among undergraduates. *Social Indicators Research*, 101(1), 155-172.
- Owens, J., & Hawkins, E. (2019). Using online labor market participants for nonprofessional investor research: A comparison of mturk and qualtrics samples. *Journal of Information Systems*, 33(1), 113-128.
- Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 623-656.
- Pham, H., El-Den, J., & Richardson, J. (2016). Stress-based security compliance model—an exploratory study. *Information & Computer Security*.
- Pham, H., Brennan, L., & Furnell, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications* 46, 96-107.
- Podsakoff, LePine, & LePine. (2007). Differential challenge stressor-hindrance stressor relationships with job attitudes, turnover intentions, turnover, and withdrawal behavior: a meta-analysis. *Journal of Applied Psychology*, 92(2), 438.
- Podsakoff, P., MacKenzie, S., Lee, J., & Podsakoff, N. (2003). common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879.
- Polites, G., Roberts, N., & Thatcher, J. (2012). Conceptualizing models using multidimensional constructs: A review and guidelines for their use. *European Journal of Information Systems*, 21(1), 22-48.
- Posey, C., Bennett, R., & Roberts, T. (2011). Understanding the mindset of the abusive insider: An examination of insiders’ causal reasoning following internal security changes. *Computers & Security*, 30(6), 486-497.

- Posey, C., Roberts, T., Lowry, P., & Hightower, R. (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.
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(2), 757-778.
- Ragu-Nathan, T., Tarafdar, M., Ragu-Nathan, B., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research, 19*(4), 417-433.
- Rhee, H., Kim, C., & Ryu, Y. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.
- Ringle, C., Wende, S., & Becker, J. (2015). *Smartpls 3. Boenningstedt: SmartPLS GmbH.*
- Robinson, S., & Bennett, R. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal, 38*(2), 555-572.
- Rodell, J., & Judge, T. (2009). Can "good" stressors spark "bad" behaviors? The mediating role of emotions in links of challenge and hindrance stressors with citizenship and counterproductive behaviors. *Journal of Applied Psychology, 94*(6), 1438.
- Rouse, S. (2015). A reliability analysis of mechanical turk data. *Computers in Human Behavior, 43*, 304-307.
- Sackett, P. (2002). The structure of counterproductive work behaviors: Dimensionality and relationships with facets of job performance. *International Journal of Selection and Assessment, 10*(1-2), 5-11.
- Safa, N., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451.
- Sarkar, S., Vance, A., Ramesh, B., Demestihis, M., & Wu, D. (2020). The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Information Systems Research.*
- Schaufeli, W., & Bakker, A. (2004). Job demands, job resources, and their relationship with burnout and engagement: A multi-sample study. *The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 25*(3), 293-315.

- Schaufeli, W. (2017). Applying the job demands-resources model. *Organizational Dynamics*, 2(46), 120-132.
- Schaufeli, W., & Taris, T. (2014). A critical review of the job demands-resources model: Implications for improving work and health. *Bridging Occupational, Organizational and Public Health*, 43-68.
- Selye, H. (1974). *Stress without distress*. J.B. Lippincott Co.
- Shih, S., Jiang, J., Klein, G., & Wang, E. (2013). Job burnout of the information technology worker: Work exhaustion, depersonalization, and personal accomplishment. *Information & Management*, 50(7), 582-589.
- Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, 177-191.
- Simmons, B., & Nelson, D. (2001). Eustress at work: The relationship between hope and health in hospital nurses. *Health Care Management Review*, 26(4), 7-18.
- Simmons, B. L., & Nelson, D. L. (2007). Eustress at work: Extending the holistic stress model. *Positive Organizational Behavior*, 40-53.
- Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*.
- Sommer, S., Howell, J., & Hadley, C. (2016). Keeping positive and building strength: The role of affect and team leadership in developing resilience during an organizational crisis. *Group & Organization Management*, 41(2), 172-202.
- Spector, P., & Fox, S. (2010). Counterproductive work behavior and organisational citizenship behavior: Are they opposite forms of active behavior? *Applied Psychology*, 59(1), 21-39.
- Spector, P., Fox, S., Penney, L., Bruursema, K., Goh, A., & Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviors created equal? *Journal of Vocational Behavior*, 68(3), 446-460.
- Spector, P., & Fox, S. (2005). The stressor-emotion model of counterproductive work behavior. In S. Fox & P. E. Spector (Eds.), *Counterproductive work behavior: Investigations of actors and targets*, American Psychological Association.
- Spector, P., Dwyer, D., & Jex, S. (1988). Relation of job stressors to affective, health, and performance outcomes: A comparison of multiple data sources. *Journal of Applied Psychology*, 73(1), 11.

- Steelman, Z., Hammer, B., & Limayem, M. (2015). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, 39(2).
- Spitzer, D. (2020). IT security consulting in the U.S. *IBIS World Industry Report*.
- Sykes, A. (2015). Support structures and their impacts on employee outcomes: A longitudinal field study of an enterprise system implementation. *MIS Quarterly* 39(2).
- Tams, S., Thatcher, J., & 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., & Ragu-Nathan, T. (2014). Examining impacts of technostress on the professional salesperson's behavioural performance. *Journal of Personal Selling & Sales Management*, 34(1), 51-69.
- Tarafdar, M., Cooper, C., & Stich, J. (2017). The technostress trifecta-techno eustress, techno distress and design: Theoretical directions and an agenda for research. *Information Systems Journal*, 29(1), 6-42.
- Tarafdar, M., Pullins, E., & 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, T. (2010). Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems*, 27(3), 303-334.
- Tarafdar, M., Tu, Q., Ragu-Nathan, T., & Ragu-Nathan, B. (2011). Crossing to the dark side: Examining creators, outcomes, and inhibitors of technostress. *Communications of the ACM*, 54(9), 113-120.
- Tehseen, S., Ramayah, T., & Sajilan, S. (2017). Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences*, 4(2), 142-168.
- Thomson, M., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, 6(4), 167-173.
- Thompson, N., McGill, T., & Wang, X. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. *Computers & Security*, 70, 376-391.
- Trevino, L. (1992). Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly*, 121-136.

- Wang, J., Li, Y., & Rao, H. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, 28(2), 378-396.
- Watson, D., Clark, L., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: The panas scales. *Journal of Personality and Social Psychology*, 54(6), 1063.
- Weiss, M. (1983). Effects of work stress and social support on information systems managers. *MIS Quarterly*, 29-43
- Whitman, M., Townsend, A., & Aalberts, R. (2001). Information systems security and the need for policy in information security management: Global challenges in the new millennium. *IGI Global*, 9-18.
- Wolter, C., Santa Maria, A., Wörfel, F., Gusy, B., Lesener, T., Kleiber, D., & Renneberg, B. (2019). Job demands, job resources, and well-being in police officers: A resource-oriented approach. *Journal of Police and Criminal Psychology*, 34(1), 45-54.
- Xu, F., Luo, X., & Hsu, C. (2019). Anger or fear? Effects of discrete emotions on employee's computer-related deviant behavior. *Information & Management*, 103-180.
- Yoo, C., Sanders, G., & Cervený, R. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, 108, 107-118.
- Yu, L., Cao, X., Liu, Z., & Wang, J. (2018). Excessive social media use at work: Exploring the effects of social media overload on job performance. *Information Technology & People*.
- Zafar, H., & Clark, J. (2009). Current State of Information Security Research in IS. *Communications of the Association for Information Systems*, 24(1), 34.
- Zakaria, O. (2006). Internalisation of information security culture amongst employees through basic security knowledge. *IFIP International Information Security Conference*, Springer.
- Zhen, J., Xie, Z., Dong, K., & Chen, L. (2021). Impact of negative emotions on violations of information security policy and possible mitigations. *Behaviour & Information Technology*, 1-13.
- Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187.

APPENDIX A
HUMAN USE APPROVAL LETTER



LOUISIANA TECH
UNIVERSITY.

OFFICE OF SPONSORED PROJECTS

MEMORANDUM

TO: Mr. Bao Duong, Dr. Craig Van Slyke
 FROM: Dr. Richard Kordal, Director of Intellectual Property & Commercialization
 (OIPC)
rkordal@latech.edu
 SUBJECT: HUMAN USE COMMITTEE REVIEW
 DATE: Feb 12, 2021

In order to facilitate your project, an EXPEDITED REVIEW has been done for your proposed study entitled:

"Information Security Technologies - Perceptions and Practices"

HUC 21-058

The proposed study's revised procedures were found to provide reasonable and adequate safeguards against possible risks involving human subjects. The information to be collected may be personal in nature or implication. Therefore, diligent care needs to be taken to protect the privacy of the participants and to assure that the data are kept confidential. Informed consent is a critical part of the research process. The subjects must be informed that their participation is voluntary. It is important that consent materials be presented in a language understandable to every participant. If you have participants in your study whose first language is not English, be sure that informed consent materials are adequately explained or translated. Since your reviewed project appears to do no damage to the participants, the Human Use Committee grants approval of the involvement of human subjects as outlined.

Projects should be renewed annually. *This approval was finalized on February 12, 2021 and this project will need to receive a continuation review by the IRB if the project continues beyond February 12, 2022. ANY CHANGES* to your protocol procedures, including minor changes, should be reported immediately to the IRB for approval before implementation. Projects involving NIH funds require annual education training to be documented. For more information regarding this, contact the Office of Sponsored Projects.

You are requested to maintain written records of your procedures, data collected, and subjects involved. These records will need to be available upon request during the conduct of the study and retained by the university for three years after the conclusion of the study. If changes occur in recruiting of subjects, informed consent process or in your research protocol, or if unanticipated problems should arise it is the Researchers responsibility to notify the Office of Sponsored Projects or IRB in writing. The project should be discontinued until modifications can be reviewed and approved.

A MEMBER OF THE UNIVERSITY OF LOUISIANA SYSTEM

P.O. BOX 3092 • RUSTON, LA 71272 • TEL: (318) 257-5075 • FAX: (318) 257-5079

AN EQUAL OPPORTUNITY UNIVERSITY

APPENDIX B
SCREENING QUESTIONS

Screening Questions:

1. Do you depend on information technology devices (laptop, desktop, smartphone, etc.) to do your work?

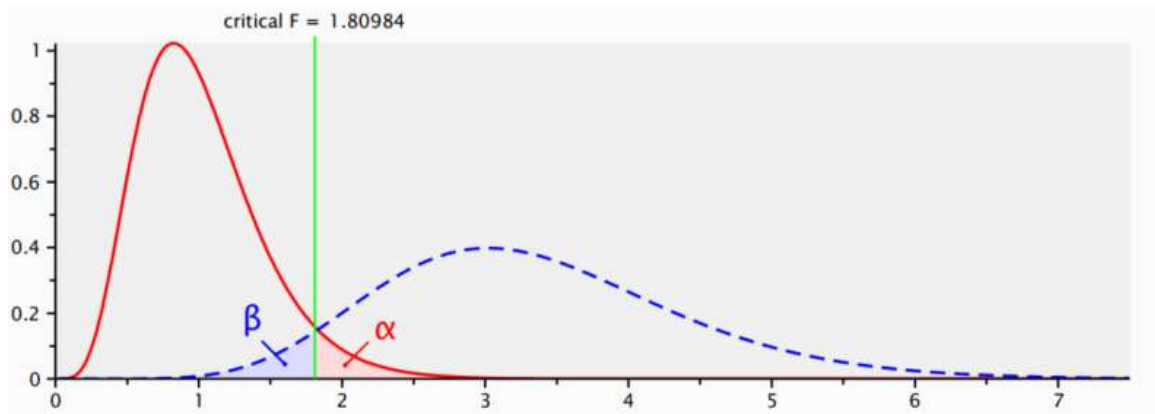
- Yes
- No

2. Does your organization have an information security policy?

- Yes
- No

APPENDIX C
POWER ANALYSIS

Power Analysis



APPENDIX D
WORKER REQUIREMENTS

Worker requirements

Require that Workers be Masters to do your tasks (What are Mechanical Turk Masters?)

Yes No

Specify any additional qualifications Workers must meet to work on your tasks:

Location UNITED STATES (US)

HIT Approval Rate (%) for all Requesters' HITs 98

(up to 3 more)

(Premium Qualifications incur additional fees; see Pricing Details to learn more.)

Project contains adult content (See Details)

This project may contain potentially explicit or offensive content, for example, nudity.

Task Visibility (What is task visibility?)

Public - All Workers can see and preview my tasks

Private - All Workers can see my tasks, but only Workers that meet all Qualification requirements can preview my tasks

Hidden - Only Workers that meet my Qualification requirements can see and preview my tasks