Spring 4-19-2019

The Informed Human Firewall: The Impact of Knowledge Dimensions on Employees' Secure Behavior

Ashraf Mady
anm9230@students.kennesaw.edu

Recommended Citation

Mady, Ashraf, "The Informed Human Firewall: The Impact of Knowledge Dimensions on Employees' Secure Behavior" (2019). *PhD in Business Administration Dissertations*. 3.
https://digitalcommons.kennesaw.edu/phdba_etd/3

THE INFORMED HUMAN FIREWALL: THE IMPACT OF KNOWLEDGE DIMENSIONS ON EMPLOYEES' SECURE BEHAVIOR

By
Ashraf Mady

A Dissertation

Presented in Partial Fulfillment of Requirements for the
Degree of
Doctor of Philosophy in Business Administration
In the
Coles College of Business
Kennesaw State University

Kennesaw, GA
2019

(BLANK FOR INSERTION OF SIGNATURE PAGE)

DEDICATION

To my wife Martha and my sons, Philip and Andrew. Your kindness and your love always motivated me. You have supported my passion to pursue the Ph.D. and provided me the perfect environment to succeed. I am forever grateful. Martha, Philip, and Andrew, this is our achievement.

To mom and dad. Thank you for your love and for everything you have done for me throughout the years. I hope I made you proud.

ACKNOWLEDGEMENTS

I would sincerely like to thank my family for their endless and unquestionable support. They inspired me every day. I also want to acknowledge my committee for their wonderful support. I want to say thank you to Dr. Gupta. There are no words to describe how amazing and wonderful his support was during this journey. He is a mentor, scholar, and a truly kind friend. His wonderful leadership skills, scholarship capacity, and kindness propelled me through every challenge and guided me to completion. I am looking forward to a life-long friendship filled with academic achievements. I want to thank Dr. Warkentin for his unparalleled quality of work and for his devotion to excellence. I am truly blessed beyond words to have had this opportunity to work with and learn from Dr. Warkentin. I also want to thank Dr. Zafar for his guidance, advice, encouragements, and for consistently being reliable. Dr. Zafar was always positive, supportive, and available. I want to acknowledge that I was blessed with such a wonderful and perfect committee.

True thanks from a heart filled with gratitude and appreciation to the Ph.D. in Business Administration program at Kennesaw State University. You have provided the best education. I am blessed to have had the opportunity to be part of such a quality program that is taught and managed by the best and the most qualified group of academic scholars. Special thanks to every professor and administrator in the program. Thank you.

I want to say thank you to my colleagues at the University of North Georgia for all the support and the encouragements.

Last but definitely not least, I want to thank the Gr8est cohort ever. Every one of you is amazing. You made this possible with your and with your genuine quality. Knowing each one of you is one of the best gifts this program has given me.

ABSTRACT

THE INFORMED HUMAN FIREWALL: THE IMPACT OF KNOWLEDGE DIMENSIONS ON EMPLOYEES SECURE BEHAVIOR

By

Ashraf Mady

Organizations implement a variety of knowledge mechanisms such as information security education, training, and awareness (SETA) programs and information security policies to influence employees' secure behavior. However, skills gained through these knowledge mechanisms have not always translated to secure behavior. Protection motivation theory (PMT) is a widely used and accepted theory in information security behavioral research. Nevertheless, information security research has not examined the impact of knowledge mechanisms on PMT psychological processes. This study explains the key psychological processes that influence employees' secure behavior and seeks to understand how organizational knowledge mechanisms influence these key psychological processes that form threats perceptions.

Drawing on the knowledge management literature, the impact of knowledge mechanisms on users' threat perceptions was conceptualized and examined across three knowledge dimensions: breadth, depth, and finesse. The research also applied construal level theory (CLT) to provide a means to measure the psychological constructs of PMT from an individual's perspective. The research conceptualizes the PMT psychological process based on the threat un-desirability and coping feasibility. The four dimensions of the psychological distance from CLT (temporal, social, spatial, and hypothetical) formed the threat un-desirability while response efficacy and difficulty formed the coping feasibility construct.

This study empirically tested the model using a multi-method approach. The first method used an experiment with 262 students to validate the CLT driven constructs and its impact on protection motivation. The second study tested the overall model, including knowledge mechanisms dimensions, across a sample of 219 industry professionals. The theoretical model was tested using a structural equation modeling (SEM) approach. Results show support that the psychological distance from the threat allows employees to perceive the personal impact of the threat. Results also support that the key psychological constructs, threat un-desirability and coping feasibility, influence employees behavioral choices.

This research offers noteworthy contributions to the literature. It provides a greater understanding of the role of knowledge dimensions to motivate compliance. The research also presented an improved model that preserves the original intent of PMT in the context information security. Finally, the research presented a generalizable and practical business approach to a traditionally technical topic.

Keywords: Information security, secure behavior, compliance, construal level theory, knowledge dimensions, protection motivation, security policies, security education and training awareness, SETA programs, information security threats.

TABLE OF CONTENTS

LIST OF TABLES

TABLE OF FIGURES

CHAPTER 1 – INTRODUCTION

The rapid transformation of organizational critical information to digital format drastically increased the importance of information security (Moody, Siponen, & Pahnila, 2018). The motivation of employees to handle information in a secure manner has become a top organizational priority (Anderson, Vance, Kirwan, Eargle, & Jenkins, 2016). Organizations are struggling to protect their critical information from intentional and accidental information security violations committed by employees (Johnston, 2015). Consequently, organizations continue to invest in information security solutions such as intrusion detection systems, network traffic monitoring, software and network security, incident management, identity and access management (Ernst & Young, 2016). The purpose of this research is to understand how employees can be motivated to protect organizational digital assets from information security threats.

Information security is concerned with protecting information from accidental or malicious security incidents such as exposure of confidential information (threat to information privacy) (Arachchilage & Love, 2014), deletion of data (threat to information availability) (Safa, Von Solms, & Furnell, 2016), and data modification (threat to information integrity) (Sen & Borle, 2015). The threats to the confidentiality, integrity, and availability of information have evolved to include accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats (Whitman & Mattord, 2012). Security incidents may have dire consequences such as financial and legal liabilities, loss of reputation, negative economic impact, or employees’ demotivation (Bulgurcu, Cavusoglu, & Benbasat, 2010).

The growing global spending on security solutions and services was estimated to reach $86 billion in 2016 to counter the increasing impact of security incidents (Anderson et al., 2016). The damaging cost of data breaches was reported in 2017 to be larger in size than any time before, with a global average cost of $3.62 million per data breach (Ponemon Institute, 2017). A market study showed that more than half of the surveyed global organizations reported the need to increase their security budgets by at least 25% to effectively protect organizational information assets against growing threats (Kessel & Allan, 2015). However, despite the spending growth on organizational initiatives to secure information, security incidents continue to occur, and their damaging impact continue to grow (Ab Rahman & Choo, 2015; Safa et al., 2016; Willison & Warkentin, 2013). As a result, information security compliance has become a major research topic (Crossler et al., 2013) and a key managerial interest (Kappelman et al., 2017; Willison & Warkentin, 2013).

Information systems are sociotechnical networks of resources and capabilities that dynamically connect the technical and social subsystems in an organization (Chatterjee, Sarker, & Valacich, 2015; Griffith & Dougherty, 2001). Therefore, employees’ behaviors have a significant impact on information security (Herath & Rao, 2009a). Earlier approaches to secure these systems have focused primarily on technical solutions such as intrusion detection systems, firewall protection, and security systems design and implementation (Crossler et al., 2013). These technical countermeasure solutions are designed mostly to protect against external threats and are therefore often ineffective against employees' information security violations (Vance, Lowry, & Eggett, 2013). Hence, relying on technology-based solutions alone is not enough to eliminate threats to organizations (Bulgurcu et al., 2010). Surveys of major information security breaches show that most breaches are a result of insiders' threats rather than external threats (Crossler et al., 2013; Willison & Warkentin, 2013). In addition, external threats are targeting people's behaviors rather than computers to breach security (Sohrabi Safa, Von Solms, & Furnell, 2016).

Emerging literature concerned with information security advocates that the security of information systems is as much a behavioral issue as it is a technical issue (Burns, Posey, Roberts, & Lowry, 2017; Chatterjee et al., 2015; Da Veiga & Martins, 2015). Research has shown that successful information security can be achieved when organizations invest in both technical and behavioral controls (Bulgurcu et al., 2010; Chen, Ramamurthy, & Wen, 2012). Despite this, organizations continue to focus on technical controls underestimating behavioral risks (D'Arcy, Herath, & Shoss, 2014). This is particularly important because researchers estimate that nearly half of information security breaches are caused by employees from within the organization (Tsohou, Karyda, & Kokolakis, 2015). Behavioral aspects are tough to research and explain with consistency. Thus, researchers have recommended continued focus on factors to influence employees' secure behavior.

Organizations implement a variety of mechanisms to distribute knowledge to influence employees' secure behavior (Johnston, Warkentin, & Siponen, 2015). Dominant among these knowledge mechanisms are information security policies (Doherty, Anastasakis, & Fulford, 2009; Sommestad & Hallberg, 2013) and security education, training, and awareness programs (SETA) (Whitman, 2003). Practitioners and academic scholars continue to support the dominance of these organizational knowledge mechanisms to persuade employees' secure behavior (Johnston et al., 2015; Mathews, 2016; Moody et al., 2018).

Information security policies are articulated knowledge regarding the compliance with general organizational regulations and procedures to limit the discretion of subordinates (Knapp, Morris, Marshall, & Byrd, 2009). SETA programs provide information security knowledge that leads to comprehension, familiarity, and skills to manage security incidents (Safa et al., 2016). However, researchers have found that SETA programs and the creation of policies and procedures have not always translated to the desirable behavior (Safa et al., 2016; Sommestad, Karlzén, & Hallberg, 2015). Consequently, researchers have called for the need to understand how knowledge translates to behavior in a specific situation (Burns et al., 2017). In the scope of this research, the specific situation is a particular threat context. Information security threat context is the circumstances that exploit vulnerability that can cause damage to information security attributes: confidentiality, integrity, and availability (Fenz & Ekelhart, 2009). The desired behavior when dealing with any threat context (hereafter referred to as secure behavior) is the way in which employees act to protect information security attributes, which goes beyond compliance. Thus, the key overarching research question is:

How do knowledge mechanisms such as policies and SETA programs influence employees' secure behavior in a particular threat context?

To address this question, this research aims to understand the influence of policies and SETA programs on employees' psychological processes that create states and beliefs. The psychological process of any event determines individuals' behavior regarding this event (Trope, Liberman, & Wakslak, 2007). Researchers have argued the need to understand how individuals make information security related decisions (Tsohou et al., 2015). This research studies employees' psychological processes to explain how individuals make security related decisions. The degree to which people believe they have control and the ability to implement threat countermeasures plays an important role in people's perception of threat prevention (Workman, Bommer, & Straub, 2008). Also the context of the threat is relevant to the psychological state regarding the harmful outcomes (Wu, Stanton, Li, Galbraith, & Cole, 2005). Therefore, employees' psychological processes are influenced by the knowledge regarding information security threat in a specific context. The present research explores the context of the threat at the individual level as well as the organizational knowledge in order to examine employees' psychological processes.

1.1 The Context of Threat

The context of the threat could be known and addressed in security policies, known but not addressed yet in organizational policies, or unknown and ambiguous. Each threat to information systems is distinct and requires specific assessment, priority, and countermeasures (Friedman & Hoffman, 2008). Therefore, while the overall process to secure information systems might be the same, the process that describes the action from employees regarding specific threats needs be contextualized distinctly based on the specific context of the threat. Examining the context of threats to information security can clarify the circumstances that may influence employees' psychological state and how knowledge mechanisms can prepare employees to deal with threats that they may face. It is important to understand threat context to ensure that all major threats are explained and to understand the associated major countermeasures available to employees (Friedman & Hoffman, 2008). Without the contextualization of information security threats, employees may believe that they are invulnerable to threats against organizational information systems (Johnston et al., 2015).

Threats to the security of information systems can be categorized as external threats caused by hackers, competitors, and natural disasters or as internal threats caused by employees' behavior, whether malicious or accidental (Loch, Carr, & Warkentin, 1992). Human behavior can expose information systems to threats such as data breaches or the unauthorized access to sensitive and confidential information (Chatterjee et al., 2015; Ifinedo, 2012), viruses and malware can destroy critical data (Boss, Galletta, Lowry, Moody, & Polak, 2015; Posey, Roberts, & Lowry, 2015), damage or stolen computers and laptops (Siponen, Mahmood, & Pahnila, 2014), hacking, spoofing, phishing, policy violation, or opportunism for personal gain (Chatterjee et al., 2015). Also threats can come from natural disasters such as hurricanes, earthquakes, or floods that destroy organizations' infrastructures or equipment, which prevent physical access to systems or causing loss of critical data (Loch et al., 1992).

Threats can come from software infected with computer programs, called spyware, that collect data and monitor user activities (Chatterjee et al., 2015; Johnston & Warkentin, 2010). In addition, spam emails or suspicious websites can threaten data privacy and confidentiality (Ifinedo, 2012; Posey et al., 2015). Furthermore, threats from the use of unauthorized equipment or software or from violating organizational use policies can expose or destroy confidential information (Vance, Siponen, & Pahnila, 2012).

Researchers in the psychology domain found that the context of a threat influences an individual's psychological state because it explains the degree of harm associated with the threat (Wu et al., 2005). Threat context enables employees to understand and assess threats (Babar, Mahalle, Stango, Prasad, & Prasad, 2010). A user's psychological state can influence his or her evaluation and facilitate the development of favorable behavioral intentions (Ho, Ke, & Liu, 2015). Thus, this research focuses on clarifying the psychological attributes of the threat environment to distinguish between threats and to see how such attributes affects the downstream actions of an individual.

1.2 Knowledge Mechanisms: Organizational Security Policy and Training

Knowledge regarding compliance in the organization is gained by articulated processes and procedures (Sanchez, 1997) or through training (S. Gupta, Bostrom, & Huber, 2010). Information security policies and SETA programs have widely been established in the organizations as the sources for knowledge to safeguard and secure information (Chen, Ramamurthy, & Wen, 2015). Information security policies communicate compliance requirements, incidents definition, and information risk management in order to assess awareness pertaining to information protection (Da Veiga & Martins, 2015). Security policies serve as internal regulation and law with the intention to direct the behaviors of employees toward information security (Chen et al., 2015). SETA programs are procedural mechanisms implemented in the organization so that information security becomes a natural inherent aspect in employees daily jobs (Chen et al., 2015). Researchers suggested that SETA programs are recommended to enable security polices because employees need to be trained, educated, and motivated to follow security policies and procedures (Chen et al., 2015). Organizations implement security policies and SETA programs with great variations depending on various factors, such as: industry, size of the organization, degree of information intensity in the organization, and the characteristics of its employees (Bulgurcu et al., 2010). Literature shows that regardless of the knowledge sources, having adequate knowledge regarding information security is a prerequisite to performing any normal activity in a secure manner (Van Niekerk & Von Solms, 2010). Knowledge provides theoretical, strategic, and practical understanding of the available course of action (Sanchez, 1997).

Thus, instead of focusing on security policies and SETA programs directly, researchers in information security literature have advocated for focusing on knowledge dimensions, such as the comprehensiveness of knowledge (Siponen & Iivari, 2006). As a result, information security research focused mainly on the use of the comprehensiveness of knowledge without explaining whether that means depth of knowledge, breadth of knowledge, or creative use of knowledge. Information security literature currently does not explicitly leverage knowledge dimensions. To address this gap, this study draws from the knowledge management literature, as it presents a more complete picture of knowledge dimensions that are not yet explored in information security literature. Scholars studying knowledge management explained that knowledge is a multidimensional construct that provides outcomes unique to each of the knowledge dimensions (Sanchez, 1997). Knowledge dimensions are breadth, depth, and finesse

(Munro et al., 1997). Knowledge breadth is the variety of knowledge, knowledge depth represents the completeness of knowledge regarding a specific subject, and finesse is the ability to apply innovativeness and creativity (Munro et al., 1997). Breadth of information security knowledge, increases employees' security awareness and prevents duplication of efforts saving time and money (Safa et al., 2016). Depth of knowledge is required to learn how to identify a threat and know the specific steps needed to deal with that threat (Ben-Asher & Gonzalez, 2015). Finesse embodies creativity, self- sufficiency, and ability to learn new things (Mills & Chin, 2007). Overall, this research investigates the embedded knowledge dimensions (breadth, depth, and finesse) as key factors that influence employees' psychological processes and subsequent behavior.

1.3 Psychological Process

All behaviors are driven by the psychological process (Trope et al., 2007). Researchers have used various behavioral theories in the context of information security to study compliance behavior. For example, Chatterjee et al. (2015) investigated employees' attitude and subjective norms regarding security. They applied the theory of planned behavior (Ajzen, 1991). Chen et al. (2012) applied the general deterrence theory to explain the impact of punishment and deterrence mechanisms on security. Liang and Xue (2009) tested the technology threat avoidance theory (TTAT) to explain user rejection of malicious IT artifacts. Several researchers used protection motivation theory (Rogers, 1975) in the study of employees' behavioral change and focused on compliance motivation (Sommestad et al., 2015). The revised version of protection motivation theory (PMT) (Maddux & Rogers, 1983; Rogers, 1983) has been noted as one of the dominant theories for predicting individuals' intentions to engage in protective actions

(Ifinedo, 2012). PMT is used extensively to investigate behavior in the context information security (Boss et al., 2015).

This research draws on the revised version of PMT (Maddux & Rogers, 1983; Rogers, 1983) to explain the psychological processes that motivate individuals to engage in protective behavior when faced with threats. PMT postulates that individuals' motivation to protect themselves from any threat is a result of the outcome of two appraisal processes, threat appraisal and coping appraisal (Johnston & Warkentin, 2010). Threat appraisal is an individual's perception of the probability of exposure or vulnerability to a threat, as well as the perceived severity of the consequences of that threat (Boss et al., 2015; Ifinedo, 2012). Coping appraisal is the process by which individuals evaluate the feasibility of the available risk mitigating action or response efficacy, their own ability to contribute to the recommended protective response or self-efficacy, and the response cost (Posey et al., 2015).

Although PMT has been used in a sizable number of studies in the context of information security, the key variables' impact, significance, and directions have shown great variations and inconsistencies (Posey et al., 2015). Several researchers supported the positive impact of the severity of threat on compliance motivation as proposed by PMT (Sommestad et al., 2015). In contrast, other researchers reported a negative impact of threat severity (Herath & Rao, 2009b; Warkentin, Walden, Johnston, & Straub, 2016) or found its impact to be insignificant (Ifinedo, 2012). As a result, scholars argue that the context of application is a potential reason for PMT inconsistent results (Johnston et al., 2015). Researchers have called for future research to address the inconsistent findings regarding the impact of each of PMT constructs in the context of information security

(Warkentin et al., 2016). To address the inconsistencies, this research applied PMT based on its original intent that requires threats to be on a personal level and not a threat against the organization.

This research introduces an employee's psychological distance to security threats to apply PMT, as originally intended, from a personal level. Psychological distance is a personal reference regarding an event (Trope & Liberman, 2010). Psychological distance impacts the way individuals perceive events (Trope & Liberman, 2003). Overall, this research draws on psychological distance theory to dimensionalize the threat environment and then investigates how these dimensions impact the psychological process that leads to end-user behavior. Such an approach enables information security threats to be personal threats and preserves the original intention of PMT.

1.4 Specific Research Questions

This study understands how the use knowledge dimensions in SETA and security policies can motivate individuals to comply with the organization's information security regulations and procedures. The research answers the following questions:

Q1: What are the key psychological processes that influence employees' secure behavior when dealing with an information security threat?

Q2: How do organizational knowledge mechanisms such as SETA programs and policies influence key psychological processes of threat perception?

The research offers noteworthy contributions to the literature. The research develops a theoretically grounded model for information security compliance that addresses current gaps in literature. The study investigates knowledge dimensions in

SETA programs and security policies as an input to psychological process to construct personal perceptions regarding specific information security threats. The research provides greater understanding to the role of knowledge dimensions and employees' psychological state that motivates compliance. While the existing literature has successfully expanded our knowledge and understanding regarding factors influencing information security compliance, the conventional application of PMT in the field of information security caused inconsistent and conflicting results. This research presents an approach to limit results variations and allows PMT to work as designed in the context of information security.

This research provides a generalizable approach for any incident-driven behavior and a practical business approach to a topic that is typically viewed as a technical problem. Understanding the unique outcomes to each of the knowledge dimensions provides strategies regarding the use of organizational knowledge mechanisms in the context of information security. This work presents an approach to enable practitioners and scholars to establish the linkage between security needs and job demands with an approach that enables the organization to influence compliance without hindering productivity. It highlights the use of SETA programs in the organization to develop more effective and attainable information security policies and procedures.

1.5 Research Design

This research applied quantitative methods to examine the relationships between variables to address the research questions. The research empirically tested the model using two-study approach. The first study was a scenario-based experiment to answer the first research question regarding key psychological processes of threat perception. The experiment was conducted with 262 university students. Participants were provided various manipulation scenarios that represented different psychological distances. To achieve this, the researcher manipulated the degree of abstraction or concreteness of specific threat contexts. Students were asked to fill a behavioral focused questionnaire to empirically validate the instrument that measures the impact of threat un-desirability and coping feasibility on protection motivation.

The second study empirically validated the entire theoretical model, including input, process, and output. This approach was consistent with seminal information systems literature. Literature supports that instrument validation should precede the research model empirical validation (Straub, 1989). Data were collected from 219 employees across various organization with varied responsibilities and technical competences. The theoretical model was tested using structural equation modeling (SEM) approach. The findings from this study can be used in future quantitative studies in researching the design and development of training and organizational policies concerned with employees' compliance behavior.

1.6 Organization and Overview of the Dissertation Proposal

This dissertation consists of six chapters. Following this introductory chapter, which presented the topic importance and research motivation, chapter 2 offers a review of the related literature. In chapter 2, support is drawn from reported empirical results and findings relevant to the gaps outlined in chapter 1. Chapter 3 presents the research theoretical model and hypotheses. In this chapter, the research model is presented, the constructs are explained, and justifications for the hypotheses are provided. Chapter 4 discusses the research design. This chapter establishes the quantitative multi-method approaches followed to validate empirically the research model. Chapter 4 explains the measurements, sample frame, controls, and statistical procedures. Chapter 5 presents the data analysis. This chapter includes the statistical data analysis, including constructs validity and reliability. Chapter 5 also includes a comparative analysis and results comparison between the traditional PMT model and the model presented in this research. The research discussion is presented in the final chapter, chapter 6. Chapter 6 discusses the results, interpretation, research limitations, and future research directions.

CHAPTER 2 – LITERATURE REVIEW

Much of the behavioral research in the information security literature has focused on two streams of research: a) compliance behavior and b) training and policy initiatives. The relevant research findings in both these areas are summarized in this chapter. This chapter explores the information security literature and points out relevant key findings and gaps. The review of the relevant literature brings together the major findings to advance the understanding and to show how this research can address key gaps.

The chapter starts by briefly describing a framework to integrate these research streams. Next, we draw upon knowledge mechanisms, SETA and security policies, and PMT to understand existing literature. After having summarized the literature review and the gaps, the last section presents a case for expanding the existing models of investigation to address the gaps highlighted. To review the related information security literature, a broad review of seminal research was performed. This broad review focused on understanding the impact of employees' behavior on information security. Then, the review focused on employees' behavioral motivation to understand relationships among factors influencing the main overarching research question. The literature review follows a chronological order based on the foundation of the knowledge provided by previous high-impact research through the most recent publications to identify findings and gaps outlined by the current information security research.

A holistic and systematic framework to summarize the literature is the input-process-outcome framework. Input-process-outcome was proposed by Garris, Ahlers, and Driskell (2002). In this perspective, the input is instructional content, process is the development of judgement, and the output is the influenced behavior. This framework allows us to capture the key influencers towards behavior as well as understand the process through which such a behavior decision was arrived at (see Figure 1). Input represents the elements in the environment that influence the target behavior under investigation, which in this case is secure behavior. Three elements studied in the literature are a) the threat context, b) SETA programs, and c) organizational policies. The latter two factors deal with the transfer of knowledge and are mentioned as knowledge mechanisms in the figure. Process deals with an individual's cognitive and affective psychological processes involved in arriving at the behavioral choice. Research in the information security literature has focused on psychological processes. This chapter focuses on the same. The outcome represents the behavioral choice that the end-user demonstrates in the face of a threat.

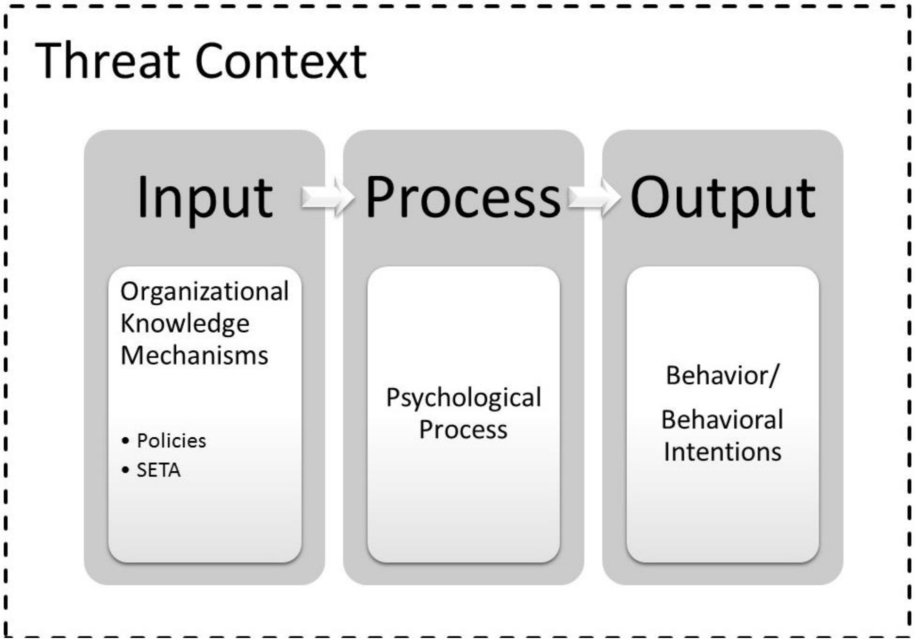

Figure 1. Literature review organization

Following the explained systematic approach, the review of information security literature first clarifies the two inputs stemming from the literature: threat context and knowledge mechanisms. The context of a threat is relevant to the impact on the individual's psychological state (Wu et al., 2005). Then the empirical research concerned with knowledge mechanisms is synthesized to understand its influence on employees' psychological processes. Finally, the applications of PMT are reviewed in the literature to explain the psychological processes that motivate employees' secure behavior in a business environment. The major findings are organized to assimilate the current state of the information security literature and to point out the gaps that need to be addressed to explain how knowledge mechanisms influence employees' psychological processes and subsequent behavior.

2.1 Inputs - Threat Context

Threat context refers to the circumstances that exploit vulnerability caused by technical, administrative, or physical weaknesses that can cause damage to information security attributes such as confidentiality, integrity, and availability (Fenz & Ekelhart, 2009). Table 1 summarizes context of information security threat in the literature. Threats to information security can be man-made or non-human threats (Loch et al., 1992), and each threat will have a certain degree of severity (Fenz & Ekelhart, 2009).

Table 1: Literature Summary of Findings Regarding Threat Context

Literature	Threats/Implied Threats
Babar et al. (2010)	Reveal identity, expose authentication, denial of service, and tampering with organization's hardware
Boss et al. (2015)	Loss of critical data and data corruption
Chatterjee et al. (2015)	Hacking, phishing, unauthorized personal use of IT artifacts
Chen et al. (2012)	Email attachments and suspicious internet sites
D'Arcy et al. (2014)	Complex and stressful security standards
Friedman and Hoffman (2008)	Malware, phishing, spoofing, loss, and theft of devices, and user policy violations
Ifinedo (2012)	Data breaches or the unauthorized access
Johnston and Warkentin (2010)	Spyware defense
Johnston et al. (2015)	Data breach
Loch et al. (1992)	Natural disasters, unauthorized access, denial of service, reverse engineering, theft of equipment, data destruction, computer viruses, or employee fault
Posey et al. (2015)	Data corruption
Siponen et al. (2014)	Damaged or stolen computers and laptops
Vance et al. (2012)	Computer viruses and unauthorized access to confidential information
Whitman (2003)	Malicious software, system failure, mistakes, denial of service, natural disasters

Threats to information exist and are inevitable, whether or not perceived by the individual (Johnston & Warkentin, 2010). The literature suggests that there can be many types of threats, ranging from man-made or non-human threats (Loch et al., 1992). Researchers found that the most impactful man-made threats are malicious software, system failure, and employees errors whether intentional or accidental (Whitman, 2003). Researchers also addressed non-human security threats such as natural disasters like earthquakes, floods, wildfires, or hurricanes that can destroy or prevent access to information systems (Loch et al., 1992).

Threats to the security of information were also classified based on the impact on business processes. Babar et al. (2010) described three threat categories: identification, communication, and physical threats. Identification threats are the threats that reveal the identity and the authentication process for device, user, or session. Denial of service is an example of a communication threat. The physical threats include theft of equipment, facility destruction, tampering with organization's hardware, or product reverse engineering. Also, studies of information security threats addressed the dilemma of ethics and the ethical use of IT artifacts. Unauthorized personal use of IT artifacts influenced by opportunism and personal gain is an example of a threat to the security of information systems caused by the unethical use of information systems (Chatterjee et al., 2015). Finally, information security research has identified sixty-seven unique protection-motivated behaviors for employees to follow in the organization (Posey, Roberts, Lowry, Bennett, & Courtney, 2013).

This extensive focus on threat context has resulted in researchers focusing on compliance behavior, e.g., better management of passwords (Chen et al., 2012; Ifinedo, 2012; Johnston et al., 2015), use of an encrypted USB drive, or locked workstations (Johnston et al., 2015; Posey et al., 2015) to prevent data breaches. Such research, however, does not focus on the process through which an end user understands and deals with the threat. The operation of a threat has been often inferred from its effects rather than the direct assessment of the threat itself (Branscombe, Ellemers, Spears, & Doosje, 1999). As a result, the research provided sixty-seven different behavioral solutions influenced by information security threat effects (Posey et al., 2013) resulting in threat interpretational difficulties (Branscombe et al., 1999). Threats to the security of the information are distinct and require specific assessments and behavior judgments by the end-user (Friedman & Hoffman, 2008).

In this research, instead of focusing on specific threat types, the focus is on how any threat is perceived by the end-user. This allows the research to be generalizable across different threat contexts. Furthermore, it provides additional relevance for the study because threats continue to evolve over time (Whitman, 2003).

2.2 Inputs - Knowledge Mechanisms: Policies and SETA

Extant literature suggests that comprehensive security controls in the organization rely on security education, training, and awareness (SETA) programs (Whitman, 2003), as well as policies that provide series of guidelines and procedures relating to the prevention, detection, and correction cycle of information security management (Chen et al., 2015).

Researchers described information security policies as important technical oriented documents implemented in the organization to proactively safeguard corporate information resources and reduce security breaches (Doherty et al., 2009; Ifinedo, 2012).

Information security policies were applied to communicate general rules regarding compliance requirements (Knapp et al., 2009) and to identify information risk management process in order to assess awareness pertaining to information protection (Da Veiga & Martins, 2015). Policies safeguard against information abuse, destruction and misuse (Safa et al., 2016). They were described as a useful mechanism for shaping or influencing employees' behaviors with respect to the use of organizational resources (Ifinedo, 2012). Researchers identified security policies as internal regulation and law intended to modify employees' behaviors toward information security (Chen et al., 2015; Vance et al., 2013) through the communication of compliance requirements and employees' responsibilities to protect organizational information and technology resources (Bulgurcu et al., 2010; Tsohou et al., 2015).

Researchers explained that SETA programs are procedural mechanisms implemented in the organization to manifest information security policy requirements (Da Veiga & Martins, 2015) so that information security becomes a natural inherent aspect in employees' daily jobs (Chen et al., 2015). The three elements of SETA are education, training, and awareness (Posey et al., 2015; Whitman, 2008). SETA programs were applied to communicate goals, expectations, and procedures designed for employees to encourage their information security compliance behavior (Johnston et al., 2015). Literature proposed the use of SETA as a strategy to promote information security compliance and minimize accidental security breaches (Warkentin et al., 2016). SETA programs were used to aid individuals to form the desired security perception (Tsohou et al., 2015). Researchers have suggested that SETA programs could complement policies and develop awareness of safe and ethical use (Chatterjee et al., 2015). Trained employees were found to be more positive regarding security requirements than untrained employees (Da Veiga & Martins, 2015). Table 2 below summarizes literature suggestions regarding information security policies and SETA programs.

Table 2: Literature Summary of Findings Regarding Policies and SETA

Research	Security Policies	SETA Programs	Findings
Bulgurcu et al. (2010)	Define rules and employees' responsibilities to safeguard information	Highlight compliance drivers and simplify policy requirements	Policies and SETA have a positive impact, mediated by beliefs, on security attitude toward compliance
Chatterjee et al. (2015)	Defines acceptable use of IT artifacts	Provide moral education and awareness of safe and ethical use	Results imply the negative impact of Policies and SETA on intentions for unethical use of IT artifacts
Chen et al. (2015)	Internal vision, regulations, and law regarding the security of organizational information	Mechanisms to ensure employees' awareness of information security policies	Results support the positive impact of SETA on policy awareness.
D'Arcy, Hovav, and Galletta (2009)	Define rules and guidelines for the proper use of organizational information systems	SETA programs provide knowledge to ensure the success of security policies	Policies and SETA programs deter intentions of information systems misuse
Da Veiga and Martins (2015)	Sets security regulatory requirements	Manifest information security policy requirements	Results support that security training improves information protection

Doherty et al. (2009)	Business document placed to proactively safeguard the availability, confidentiality and integrity of corporate information resources	Without SETA security policies are dead	Breadth of the existing policies is modest and highly techno-centric
Ifinedo (2012)	Organizational document that outlines rules, guidelines, and requirements that must be met to safeguard IS assets	Can increase policy compliance	Researcher Suggests that SETA can have a positive impact on compliance
Johnston et al. (2015)	Recommended secure behavior	Articulate and communicate security goals and expectations	Results imply the positive effect of SETA on policy compliance
Knapp et al. (2009)	The single most important control to protect valuable information First step towards the protection of valuable information	Promote favorable security practices	Policies are ineffective without enforcement and SETA promote secure practice
Posey et al. (2015)	Organizational rules and regulations for organizational security	Provide the foundation for the appraisals of threats and available responses	SETA programs have a significant positive impact on response efficacy
Safa et al. (2016)	Address information risks and safeguard against information abuse, destruction, and misuse	Intervention strategy for information security	Training has a positive effect on attitudes toward compliance
Tsohou et al. (2015)	Define what is expected of individuals	Aim to produce certain security skills and competencies	SETA programs promote security compliance

Vance et al. (2013)	Internal regulation to control access to information	Training can prevent policy violations and bring awareness to policy requirements	Awareness has a negative impact on intentions to commit access violation
Warkentin et al. (2016)	Persuasive communication through fear appeals to motivate compliance	Support and reinforce security policies	Results imply that SETA programs are effective in encouraging protective behavior

Overall, the research in this area shows that training and organizational policy mechanisms have a positive impact, highlighting the importance of these two mechanisms (Chen et al., 2015). An additional conclusion that can be derived from the above table is that the both policy and training have a similar impact. Both serve as knowledge transfer mechanisms (Da Veiga & Martins, 2015). Researchers have generally treated training and policy-based models as an input-output model, thus ignoring the critical role of process (Tsohou et al., 2015). Transforming security behavior goes beyond the communication and acquisition of knowledge and awareness of threats and security (Johnston et al., 2015). Researchers have argued that in order for knowledge mechanisms to succeed, there is a need to have a deeper understanding of the individuals' process of information that stimulates behavioral change (Warkentin et al., 2016). An understanding of the influence that training and policy have on key process constructs will help trainers and researchers better design training and write policies. Additionally, as can be seen from Table 2, there is great variation in policies and training across research and organizational contexts. Also, each individual might interpret these mechanisms differently. This has resulted in variations in impact (D'Arcy et al., 2009; Warkentin et al., 2016). This results in a lack of generalizability of the results.

In this research, instead of focusing on the effectiveness of specific policy and training, the focus is on the knowledge dimensions that these mechanisms embed. Information security researchers have addressed the comprehensiveness as the only dimension (Siponen & Iivari, 2006). However, knowledge management perspectives see knowledge as a multidimensional construct (Sanchez, 1997). The three independent dimensions of knowledge that shape employees' abilities are breadth, depth, and finesse (Munro, Huff, Marcolin, & Compeau, 1997). Knowledge breadth is the horizontal dimension that captures the understanding of a varied and diverse range of information and factors (Luca & Atuahene-Gima, 2007). Knowledge depth represents the completeness of the user's knowledge that leads to mastery of a particular subject or task while finesse is the ability to apply innovativeness and creativity (Munro et al., 1997). These three dimensions have been studied in the knowledge management literature and help explain comprehensiveness better. These dimensions exist across all trainings and policies (although in different levels) and thus, they provide the ability to account for variance across policies and training. The application of knowledge across these three dimensions also helps in providing guidelines that are more specific to practitioners.

2.3 Process - Psychological Process

PMT has become a dominant theoretical foundation used to investigate behavior in information security (Boss et al., 2015; Crossler et al., 2013; Herath & Rao, 2009b). PMT argues that intentions are motivated by individuals' assessment of threats based on two cognitive processes, the threat appraisal and coping appraisal (Johnston &

Warkentin, 2010) and is thus used to summarize this section. PMT was originally developed for disease prevention and health promotion (Floyd, Prentice-Dunn, & Rogers, 2000). The theory was developed to explain the effects of fear appeals on health attitudes and protective behavior (Rogers, 1975). The theory was revised, Figure 2, to include a broader range of factors and became a general model of attitude change (Maddux & Rogers, 1983; Norman, Boer, & Seydel, 2005; Rogers, 1983). As indicated in the previous chapter, this research drew on the revised version of PMT (Maddux & Rogers, 1983; Rogers, 1983). In this section, PMT was used to organize existing literature, pointing out some major findings and gaps.

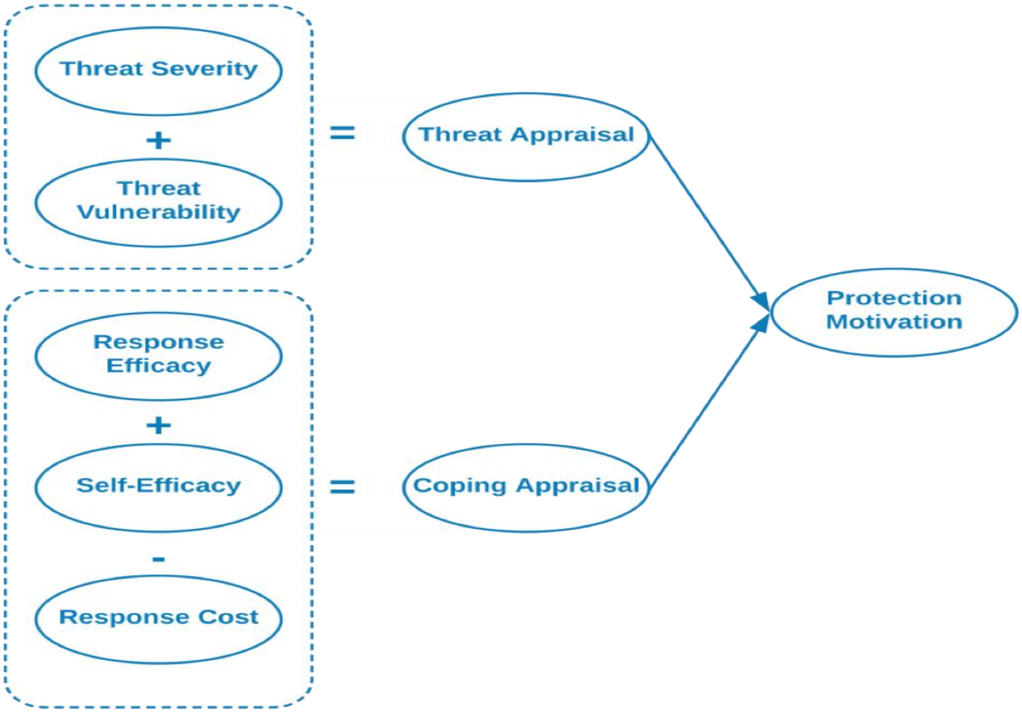

Figure 2. Diagram of the modified protection motivation theory

2.4 Threat Appraisal

Threat appraisal is the individual's assessment of the probability of exposure or vulnerability and the assessment of the severity of that threat (Ifinedo, 2012). Table 3 summarizes research findings regarding the application of threat appraisal constructs and the impact on employees' behavioral intentions. The table shows threat appraisal constructs that were tested and the constructs that were not included in the summarized literature. The table also shows whether the tested threat appraisal constructs reflected positive, negative, or insignificant impacts on compliance intentions. Each component is discussed next.

Table 3: Literature Summary of Findings Regarding Threat Appraisal Impact on Behavioral Intentions

Literature	Threat Severity	Threat Vulnerability	Context
Boss et al. (2015)	Positive impact when perceived on a personal level	Positive impact when applied only on personal level	Systems and information backup and the use of anti-malware software
Bulgurcu et al. (2010)	Positive impact	Positive impact	Organizational information security policy compliance
Chen et al. (2012)	Positive impact	Not included	Password management, email attachments, and suspicious internet sites
Herath and Rao (2009a)	When conceptualized through severity of punishment had a negative impact on compliance	Not included	Detection of employees' policy violations
Herath and Rao (2009b)	Positive impact	Not supported	Security breach that leads to denial of service and loss of data

Ifinedo (2012)	Not supported	Positive impact	Information access control, downloading illegal software and freeware
Johnston and Warkentin (2010)	Positive impact	Not supported	Spyware defense
Johnston et al. (2015)	Positive impact when applied only on personal level	Positive impact when applied only on personal level	Theft of password, login information, or unencrypted USB drive
D. Lee, Larose, and Rifon (2008)	Not Supported	Positive impact	Antivirus protection
Y. Lee and Larsen (2009)	Positive impact	Positive impact however, relatively weaker than expected	The adoption of antimalware software
Posey et al. (2015)	Positive impact when applied only on personal level	Not Supported	Protection from unauthorized login, protecting stored data, appropriate use of email and Internet, software updates
Siponen et al. (2014)	Positive impact	Positive impact	Locking office doors, turning off PCs at the end of the day, and password protection
Vance et al. (2012)	Positive impact	Not supported	Sharing passwords, failing to lock or log off a workstation, allowing reading confidential material at printers
Warkentin et al. (2016)	Positive impact	Positive impact when applied only on a personal level and organization vulnerability was not supported	Use of encryption to protect data, careful when opening attachment, perform security updates, perform antivirus scans frequently, change password frequently, lock

			the computer, back up regularly

Threat severity is an individual's perception regarding the level or the degree of the damaging impact of the threat (Sommestad et al., 2015). In the context of information security policy compliance, it refers to the evaluation of the severity of the damage and the possible negative events resulting from noncompliance with the recommended information security policies (Vance et al., 2012). The behavior of individuals is influenced by their appraisal of the damaging impact of a threat and its unwarranted consequences (Sommestad et al., 2015). The overall assessment of severity of the threat is conceptualized to exert significant positive influence on an employee's attitude toward compliance (Bulgurcu et al., 2010; Siponen et al., 2014). However, researchers have also found a limited or even negative impact of threat severity on compliance intention in certain contexts. For example, Herath and Rao (2009a) conceptualized threat severity by the increased deterrent effect of severity of punishment. They found that severity of punishment had a negative effect on compliance intentions. To explain the results, they argued that the excessive use of punishment would create hostile, stressful, and disruptive work environment. Warkentin et al. (2016) also supported that threat severity negatively impacts compliance intentions and argued that the exposure to too much fear would generate stress, resulting in a behavior that is oriented towards alleviating that fear rather than dealing with the threat itself. Other researchers have addressed the importance of the context of application on perception arguing that the threat severity will have a positive impact on compliance intentions only in a personal context (Boss et al., 2015).

Threat vulnerability is the extent of being susceptible to damage caused by information security risks (Anderson et al., 2016). The persuasive communication of the person's vulnerability to the threat is used to deliver fear that will motivate individuals to comply with the recommended protective response (Boss et al., 2015). Researchers found vulnerability to security threats to have a significant impact on behavioral intentions toward compliance (Johnston et al., 2015). Researchers also conducted experimental research that produced results which show that in order for threat vulnerability to positively influence compliance behavior, the vulnerability must be on a personal level and not toward the organization (Warkentin et al., 2016).

However, other researchers reported conflicting results regarding the impact of vulnerability on behavioral intentions. Researchers found threat vulnerability to have an insignificant impact on protection motivation (Posey et al., 2015; Vance et al., 2012). These results are inconsistent with PMT. Researchers explained that individuals often believe that they are invulnerable to threats, and others are more vulnerable to threats than themselves with the naïve perception that bad things happen to other people (Johnston & Warkentin, 2010) or because they are overconfident and feel protected by the organizational systems (Y. Lee & Larsen, 2009). Literature also shows vulnerability had an insignificant impact on attitude towards compliance; however, the threat was contextualized on the organizational level instead of the individual level (Herath & Rao, 2009b).

Overall, a review of threat appraisal research in information security behavior has found considerable variance in results. Researchers have suggested this is primarily due to the context of the studies and have called for greater contextualization of the theory itself (Johnston et al., 2015). Additionally, the second order nature of threat appraisal has never really been questioned. These constructs originally came from an economic process model and were then applied to a variance model. This created issues regarding consistency, reliability and accuracy of measures. As a result, researchers keep adding new constructs like commitment and maladaptive rewards to increase results consistency. In this research, we suggest that threat appraisal should be re-conceptualized by grounding it in the context. This new construct allows researchers to better measure it as a psychological variable and more clearly explain the underlying psychological process.

2.5 Coping Appraisal

The coping appraisal is the process by which individuals evaluate how effective, manageable, and feasible the available risk mitigating response can be (Ifinedo, 2012). The components of coping appraisal are self-efficacy, response efficacy, and response cost (Boss et al., 2015). Table 4 summarizes the research findings regarding the application of coping appraisal constructs. The table shows which coping appraisal constructs were tested and which constructs were not included in the summarized literature. The table also shows whether the tested coping appraisal constructs reflected positive, negative, or insignificant impacts on compliance intentions. Each component is discussed next.

Table 4: Literature Summary of Findings Regarding the Use of Coping Appraisal

Literature	**Response Efficacy**	**Self-efficacy**	**Response Cost**	**Context**
Boss et al. (2015)	Study 1 – No impact	Study 1 – No impact	Negative impact	Systems and Information Backup

	Study 2 - Positive impact	Study 2 - Positive impact		and the use of anti-malware software
Bulgurcu et al. (2010)	Not included	Positive impact	Negative impact	Organizational information security policy compliance
Chatterjee et al. (2015)	Not included	Negative impact	Negative impact	Unauthorized access or software download
Ifinedo (2012)	Positive impact	Positive impact	Not supported	Information access control, downloading illegal software and freeware
Johnston and Warkentin (2010)	Positive impact	Positive impact	Not included	Use of anti-spyware
Johnston et al. (2015)	Positive impact	Positive impact	Not included	Change to complex password, encryption of USB drive loss and logging off or locking workstations
D. Lee et al. (2008)	Positive impact	Positive impact	Not included	The use of virus protection to protect online activities from virus infection
Y. Lee and Larsen (2009)	Positive impact	Positive impact	Negative impact	The adoption of antimalware software
Posey et al. (2015)	Positive impact	Not supported	Negative impact	Protection from unauthorized login, protecting stored data, appropriate use of email and Internet, software updates

Siponen et al. (2014)	Positive impact	Positive impact	Negative impact	Locking office doors, turning off PCs at the end of the day
Warkentin et al. (2016)	Positive impact	Positive impact	Negative impact	Use of encryption to protect data, careful when opening attachment, perform security updates, perform antivirus scans frequently, change password frequently, lock the computer, back up regularly

Response efficacy is the belief that the available mitigating response will work and can successfully diminish the threat (Floyd et al., 2000). Witte (1992) explains that efficacy exists as an environmental or message cue, which refers to the effectiveness of the recommended response. The perceived response efficacy refers to an individual's beliefs as to whether a defined action effectively mitigate the threat. Information security literature reflects the positive impact of response efficacy on compliance intentions. Researchers continue to debate the influence of response efficacy. Some researchers found that industry type plays a significant role to determine the degree of its impact (D. Lee et al., 2008) or reported different results based on the context of the threat (Boss et al., 2015). Others reported results consistent with PMT propositions (Johnston et al., 2015; Siponen et al., 2014). Researchers also argued factors that would impact the significance of response efficacy. Ifinedo (2012) argued that response efficacy was enabled by employees' relevant knowledge, competence, and capability to implement preventative security measures. Warkentin et al. (2016) recommended that response efficacy is more appealing when the mitigating task relative to personal goals and aligned with individuals' abilities.

Self-efficacy is the degree to which individuals believe in their own abilities to perform what is required to avert the threat (Floyd et al., 2000). Researchers have argued that self-efficacy is the single biggest predictor of behavioral change in individuals (Bandura, 1977). Information security literature supports the significant positive impact of self-efficacy on compliance intentions (Bulgurcu et al., 2010; Ifinedo, 2012). Warkentin et al. (2016) argued that self-efficacy had the strongest positive impact to influence compliance intentions. However, other researchers argued factors that can weaken or even diminish the impact of self-efficacy on compliance. For example, D'Arcy et al. (2014) argued that the increased complexity of security policy requirement would have a negative impact on self-efficacy. Other researchers could not even validate the impact of self-efficacy on compliance intentions (Posey et al., 2015). On the contrast to prior findings, Chatterjee et al. (2015) suggested that self-efficacy is negatively associated with ethical use because it enables employees to manipulate technology maliciously.

Response cost is mainly the extra time and efforts needed to mitigate the risk (Ifinedo, 2012; Sommestad et al., 2015). The literature generally agreed on the significant negative impact of response cost on compliance (Boss et al., 2015; Herath & Rao, 2009b). However, Ifinedo (2012) and D. Lee et al. (2008) found no support for the impact of response cost on compliance. More researchers focused on different factors that can impact the evaluation of response cost. D'Arcy et al. (2014) confirmed that the increased security demands would increase the cost of compliance. Other researchers asserted that cost of compliance is calculated as lack of productivity (Bulgurcu et al., 2010; Posey et al., 2015). Existing literature has also showed that not only time and efforts impact cost of compliance, but also the loss of business opportunities will cause response cost to be perceived significantly higher (Posey et al., 2015; Siponen & Iivari, 2006). Our reading of the literature shows that when the response cost is measured at an individual level, the results are positive.

Overall, the extant research shows significant variance in the impact of cost appraisal factors on protection motivation. Additionally, researchers have defined components of cost appraisal differently (D'Arcy et al., 2014; Posey et al., 2015), which leads to construct validity issues. Finally, response efficacy and self-efficacy have been defined at the task level, rather than at the threat level. This is inconsistent because a user might have multiple means of mitigating the threat (S. Gupta et al., 2010).

In this study, we re-conceptualized the intent of coping by focusing on the individual’s perception of the task to be performed. This study removed all components that are task-irrelevant and focused on the perception of the effort required for the coping mechanism. Similar to threat appraisal reconceptualization, this also helps move the construct from an economic model brought to behavioral research to a psychological construct in behavioral research.

2.6 Outcome - Behavioral Intentions

The primary focus of PMT is to predict behavior. It contends that protection motivation is the primary driver of such behavior (Boss et al., 2015; Maddux & Rogers, 1983). Protection motivation reflects the individual’s intentions to engage in protective behavior (Johnston et al., 2015). Much of the focus of existing research has been on compliance behavior (See table 3-4). Compliance behavior or conformation to established rules and standards assumes that well defined ways of handling known threats. This might not be true. Additionally, it focuses on a perceived (and prescribed) solution rather than on mitigating the threat. Studying behaviors as isolated events can inhibit researchers' understanding of the complex psychological processes surrounding the overall superset of human behaviors (Posey et al., 2013). In this research, the focus is on secure behavior instead of compliance. We conceptualized secure behavior as being a superset of compliance behavior, also encompassing actions that a user might see fit in case of threat.

2.7 Chapter Summary

In sum, this chapter presented a literature review of extant literature in information security training and behavior. The review showed the variance in training and policies between studies. This highlighted the need to have an overarching framework to understand and compare different types of training / policy from a user's perspective. The review also highlighted the inconsistent results regarding threat appraisal and coping appraisal. Additionally, the review also highlighted the fact that different components of PMT were conceptualized at different levels, i.e., task, context, and individual. All of this emphasized the need to re-conceptualize the psychosocial process.

The next chapter presents a model addressing these concerns. The model uses an established multi-dimensional view of the knowledge mechanisms (training/policy). This allows the researchers to examine distinctly each dimension and its impact. Next, the psychological processes that drive behavior are conceptualized at the threat level, which provides a consistent framework across the study.

CHAPTER 3 – THEORETICAL DEVELOPMENT

This chapter presents the research model for this study. It builds on the findings and the gaps identified in the previous chapter, and outlines how the identified gaps were addressed in the model. An overview of the research model is presented first. Next, the various constructs of the model are discussed. Theoretical arguments and testable hypothesis are presented for each causal link. Appropriate research is cited where necessary. The chapter ends with an overview of the research method proposed to test the model.

3.1 Research Model

The overarching question for this research is concerned with understanding the way knowledge mechanisms can influence employees' secure behavior in a particular threat context. The research model presented, shown in Figure 3, builds on the input-process-output framework outlined in the earlier chapter. Threat context represents the events or conditions that expose information systems to potential threats. The model conceptualized training and policy (knowledge mechanism) across three dimensions: breadth, depth, and finesse. The psychological process preserved the intent of protection motivation theory (PMT) while re-conceptualizing the constructs based on the threat un-desirability and coping feasibility. Threat un-desirability is the perception of the degree to which an individual will personally be affected by the threat. Coping feasibility is the evaluation of ease or difficulty in implementing a threat mitigating action. The model followed PMT premise where the protection motivation is influenced by the perception of threat and the available coping mechanisms. Protection motivation refers to the desire and willingness that directs activities (Floyd et al., 2000). The model also shows that protection motivation is a predictor of secure behavior.

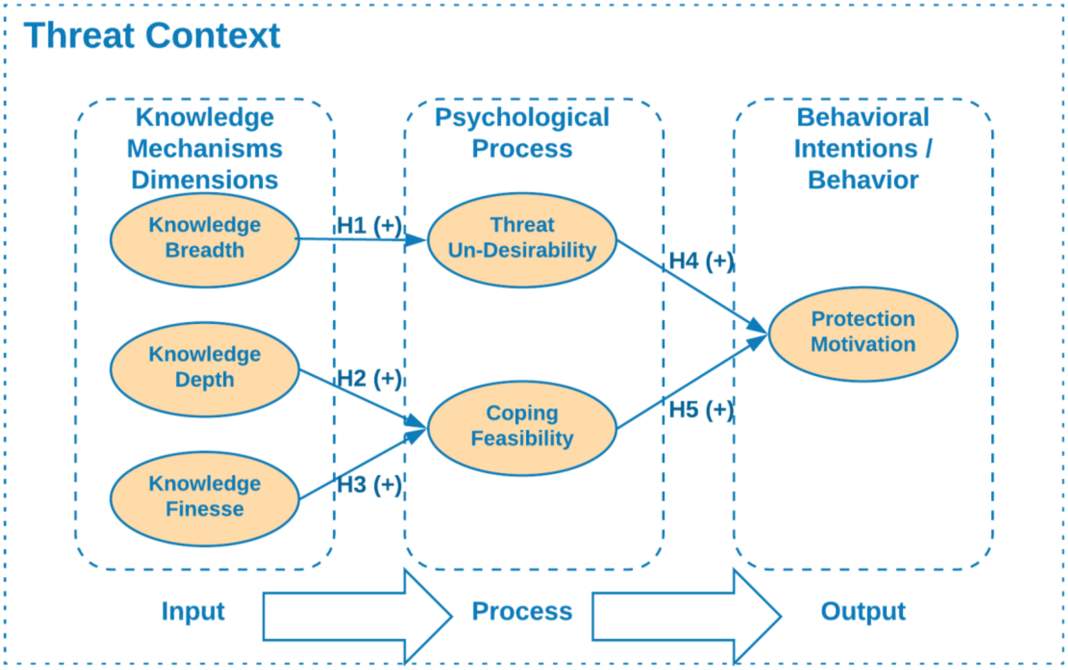

Figure 3. Research conceptual model

3.2 Threat Context

Threat context is the circumstances faced by end-users that can expose or take advantage of the technical, administrative, or physical conditions to threaten the security information confidentiality, integrity, and availability (Fenz & Ekelhart, 2009). Previous researchers have either focused on an implicit threat; thus, focusing on a specific solution (Branscombe et al., 1999; Posey et al., 2013) or researchers have focused on an objective threat limiting the research generalizability (Chatterjee et al., 2015). The consideration of threat context determines how any threat is perceived by the end-user. This allows the research to be generalizable across different known threats, as well as applicable to new threats that may emerge in the future.

This research proposes that the threat is activated through perceptions in attitude. Thus, consistent with protection motivation theory, the present research argues, in a behavioral model, that threats are manifested as artifacts of attitudes. Consequently, the proposed model is threat agnostic, i.e., the threat is generalizable across all objective threats. This research argues that it is not the objective threat, but the perception of threat by the end user, that drives the behavior. Thus, threat context is the basis of all other constructs in the model.

3.3 Knowledge Mechanism Dimensions

Knowledge is available to the organization as policies and training (Safa et al., 2016). Sanchez (1997) explained that knowledge is a multifaceted concept that provides a theoretical, strategic, and practical understanding of the available course of action. Such understanding clarifies how to perform an action, why an action provides certain results, and what the purpose of available course of action. Sanchez also suggested that each facet of knowledge has specific purposes, requires distinct communication strategies, and may impact behavior differently. Organizations aim to motivate employees with knowledge to maintain the state where security behavior is a natural behavior (Padayachee, 2012). Knowledge mechanisms convey the latest security knowledge and technical skills (D'Arcy et al., 2014). As discussed in the previous chapter, the three independent dimensions of knowledge that impact employees' abilities to perform a task are breadth, depth, and finesse (Munro et al., 1997).

Information security literature addressed the positive impact of the comprehensiveness of knowledge mechanism on employees' behaviors and suggested approaches to structure the contents of information security policy (Siponen & Iivari,

2006) and to provide effective information security training (Karjalainen & Siponen, 2011). These approaches focused on employees' cognitive process (Bulgurcu et al., 2010) to comprehend and learn about information security. The aim is to enable every organization to motivate employees to a point where security behavior is a natural behavior (Padayachee, 2012). Researchers have focused on understanding how individuals assess a topic of interest cognitively (Posey et al., 2013). However, transforming security behavior goes beyond the communication and acquisition of knowledge and awareness of threats and security (Johnston et al., 2015). Researchers advocated the need to address the gap between employees' knowledge and behaviors or the "knowing-doing" gap (Burns et al., 2017). Thus, we argue that despite the importance of cognition, behavioral drivers are affective. This research clarifies the psychological impact of knowledge mechanisms across three dimensions: breadth, depth, and finesse.

3.3.1 Breadth

Knowledge breadth refers to the different knowledge across domains with which the firm is familiar (Bierly & Chakrabarti, 1996). The breadth of knowledge is related to a broader set of tasks rather than steps of technical job requirements (Burns et al., 2017). Breadth is the horizontal dimension of knowledge (De Luca & Atuahene-Gima, 2013). In the context of information security SETA and policies, knowledge breadth can be defined as the organizational broad understanding of wide range of diverse information security threats. Information security require the coverage of wide range of organizational functions (Ashenden, 2008).

Protecting organizational information assets requires knowledge of wide range of threats and the corresponding mitigating actions (Willison & Warkentin, 2013). A policy articulates knowledge regarding general organizational rules and regulations to direct the behavior of subordinates (Knapp et al., 2009). Further, training is the most pervasive method for communicating organizations' goals (S. Gupta et al., 2010). Researchers explained that policies can be designed to reflect a broad set of risks to organizational processes (Baskerville & Siponen, 2002) and training can provide information security knowledge that leads to comprehension and familiarity to manage security incidents (Safa et al., 2016). Training has a significant impact on employees' attitude change (S. Gupta et al., 2010). Knowledge mechanisms can capture wide range of security requirements (Siponen, Baskerville, & Heikka, 2006) that leads to comprehension and familiarity (Safa et al., 2016) and increase awareness (D'Arcy et al., 2009) of security incidents and risks to information. Training goals have skill-based goals for breadth of knowledge (S. Gupta et al., 2010). Training provides theoretical principles that explain how and why training works and practical guidance for implementation (Puhakainen & Siponen, 2010). Knowledge mechanisms are used to aid individuals to form the desired security perception (Tsohou et al., 2015).

In contrast, the limited breadth of knowledge in training and policy reduces the end user's abilities to recognize threats as well as understand their impact. Researchers suggested that employees generally do not believe that their insecure behavior can make them subjected to information security threats (Vance et al., 2012). A lack of knowledge can cause accidental security breaches and can also increase security threats (Warkentin et al., 2016)

Knowledge breadth can increase employees' ability to distinguish between threats. Breadth of knowledge in knowledge mechanisms can associate employees' daily assignments with various threat contexts or the circumstances that can exploit systems' vulnerabilities and threaten the security of information. Knowledge breadth helps form adequate evaluation and understanding regarding threats' impact (Posey et al., 2015). This study argues that the breadth of knowledge can explain risks associated with wide range of security threats that users otherwise may think irrelevant to their daily responsibilities. Hence, the following hypothesis is proposed:

H1: The greater the breadth of knowledge in knowledge mechanisms, the greater the un-desirability of threat by end-users.

3.3.2 Depth

Knowledge depth is the completeness of knowledge regarding a task that leads to the competency of performance (Munro et al., 1997). Depth captures the vertical dimension of knowledge (De Luca & Atuahene-Gima, 2013). Knowledge depth is needed to address the complexity of knowledge across functional units (Galunic & Rodan, 1998). Depth provides knowledge about the capabilities of a technology (Nambisan, Agarwal, & Tanniru, 1999) and the strategic understanding of the purpose of the available course of action (Sanchez, 1997). In the context of information security, knowledge depth in knowledge mechanisms provide understanding of the complete steps needed to address any threat in a specific context. It can enable efficient and effective approach to safeguard information assets (Safa et al., 2016).

Literature shows that employees develop the desired attitude if they have the relevant expertise to implement the recommended security measures (Ifinedo, 2012). In order for employees to know how to perform any activity in a secure manner, employees would have to have sufficient knowledge to perform their tasks securely (Van Niekerk & Von Solms, 2010). Researchers suggested that information security knowledge prevents duplication of efforts, thus saving time and money (Safa et al., 2016). Literature shows that people mistakenly estimated more time on task when they had abstract knowledge which reduced task feasibility (Kanten, 2011). Having an in-depth understanding about the available course of action will increase coping feasibility.

Inadequate depth of information security knowledge is the leading cause of information security incidents created by employees (Safa et al., 2016). Abstractness about an event has a detrimental effect on accuracy (Halamish, Borovoi, & Liberman, 2017) which will increase the cost of the coping mechanism. Complex security standards can be perceived as counterproductive (Herath & Rao, 2009b). Lack of depth in knowledge mechanisms may lead employees to believe that all outcomes are predetermined and therefore, the threat impact is inevitable (Workman et al., 2008). Also, a lack of depth of knowledge may contribute to the perception of the conflict between business opportunities and security demands (Siponen & Iivari, 2006). Researchers concluded that violations are justified by the perception of counterproductive security measures (Bulgurcu et al., 2010; Posey et al., 2015). Lack of knowledge depth may cause performance delay that increases the cost of response and employees will be reluctant to comply (Anderson et al., 2016) and encourage employees to rationalize violations (Siponen & Vance, 2010).

Researchers expressed that not only is it important for employees to be aware of security measures, but also they need to be able to successfully carry out these tasks

(Padayachee, 2012). Employees need to maintain their productivity for security requirements to be feasible (Posey et al., 2015; Siponen & Iivari, 2006). Knowledge depth can allow employees to perform their daily assignment while in compliance with the organization's security requirements (Chen et al., 2015). The knowledge about feasible responses can have a positive impact on secure behavior (Warkentin et al., 2016). Security measures need to be perceived as viable to be followed (Padayachee, 2012). Therefore, this study argued that knowledge depth provides feasible approach to apply the available security recommendations. Hence, the following hypothesis is proposed:

H2: The greater the depth of knowledge in knowledge mechanisms, the higher the coping feasibility.

3.3.3 Finesse

Finesse is the ability to apply innovativeness to the available course of action (Munro et al., 1997). Finesse provides great operational value from insights and intuitions (B. Gupta, Iyer, & Aronson, 2000). This knowledge dimension embodies creativity, self-sufficiency, and the ability to learn new things (Mills & Chin, 2007). In the context of information security, finesse is the ability to follow creative approaches to mitigate a threat in a specific context. Finesse allows the mining of employees’ insights and intuitions (B. Gupta et al., 2000). Employees can be more motivated to adopt security practices if they have the skills and the experience (Padayachee, 2012).

Finesse is a dimension of knowledge that has not been considered in the context of information security. However, Studies have shown that having an innovative creative style is positively correlated with IT use (Gallivan, 2003). Knowledge can be transferred through frequent advice from experts (Galunic & Rodan, 1998) or employees’ collaboration (Safa et al., 2016). Knowledge is personalized information possessed in the mind of individuals (Alavi & Leidner, 2001). Therefore, finesse allows employees to collaborate and brainstorm to create feasible approaches to required tasks. This is consistent with Nonaka, Byosiere, Borucki, and Konno (1994), that such approach improves competence and enhances performance. Thus, we argue that finesse enables employees to increase the feasibility of security measures. Hence, the following hypothesis is proposed:

H3: The greater the finesse, the higher the coping feasibility.

3.4 Psychological Process

Much of existing literature has focused on two psychological constructs – threat appraisal and coping appraisal. However, as shown in chapter 2, the results from empirical studies have been inconsistent. A key reason for this is the lack of personalization of the theory. The premise of PMT is to motivate individuals to protect themselves from a specific personal threat (Floyd et al., 2000; Rogers, 1983). The personal motivation is influenced by the perception of the presence of an effective response that individuals can perform to protect themselves from that threat (Floyd et al., 2000). However, threats toward the organization instead of the person did not present accurately the intent of PMT, and as a result, this approach did not motivate individuals with consistency (Warkentin et al., 2016). The analysis of prior research using PMT in information security context has confirmed varied and conflicting results for reasons other than natural variation or measurement error, suggesting that the conflicting results were due to the context of the application (Sommestad et al., 2015). Researchers called for future research to address the inconsistent findings regarding the impact of each of

PMT constructs in the context of information security (Warkentin et al., 2016). In order for PMT to create the desired protection motivation, the threat must be more concrete and related to the person and not to the person's organization (Sommestad et al., 2015). Including the dimension of personal relevance is critical to preserve the original premise of PMT. Therefore, the literature presents a need for a theoretically driven re-conceptualization of PMT constructs to preserve its intent in the context of information security.

3.4.1 Construal Level Theory

Construal level theory (CLT) (Trope & Liberman, 2010) will be introduced in this section to provide means to measure the psychological constructs of PMT from an individual's perspective, i.e., personalizing them. CLT is appropriate to bring the original intent of PMT constructs to the context of information security to minimize results inconsistency regarding PMT constructs. CLT explains the way individuals construct perception and the associated behavior regarding any particular event (Ho et al., 2015; (Köhler, Breugelmans, & Dellaert, 2011). The key concept behind the theory is the idea of "Construal". The psychological term "construal" refers to the individuals' interpretation and perception of an event (construed by individuals) (Trope et al., 2007) to come up with a behavior choice.

Individuals use construal process to construct egocentric reference point, called psychological distance, to all objects and events (Trope & Liberman, 2010). Psychological distance is egocentric; its reference point is the self in the here and now, and the different ways in which an object might be removed from that point constitute different distance (Trope & Liberman, 2010). Psychological distance impacts the way individuals perceive or construe the event (Trope & Liberman, 2003). Events are construed with a higher level of abstraction as the psychological distance increases (Trope & Liberman, 2010). By contrast, the decreased psychological distance between the individual and the event leads to lower level of construal that creates more detailed, concrete, and context-specific interpretation of the event (Trope et al., 2007). CLT explains that the closer the psychological distance between individuals and an event, the more concrete the event will be construed. On the other hand, as the psychological distance increases, the more abstract the event will become (Krishna, 2012; Trope et al., 2007).

CLT posits that psychological distance has several dimensions (Trope et al., 2007): temporal (Liberman & Trope, 1998), spatial (Fujita, Eyal, Chaiken, Trope, & Liberman, 2008), social (Liviatan, Trope, & Liberman, 2008), and hypothetical (Wakslak, Trope, Liberman, & Alony, 2006). All four types of distance produced significant effects on construal level, supporting the central proposition of CLT that variation along any dimension of psychological distance will influence construal level, which means the degree of interpretation’s abstraction (Soderberg, Callahan, Kochersberger, Amit, & Ledgerwood, 2015).

The temporal dimension is a time relevant dimension that explains the psychological distance for an event that is happening now compared to an event that will happen in the future (Liberman & Trope, 1998). A spatial dimension is a place relevant dimension that explains the psychological distance for an event that will take place here compared to an event that will take place somewhere else (Fujita et al., 2008). The social dimension is a people relevant dimension that explains the psychological distance for an event that will impact the person's own-self compared to an event that will impact others (Liviatan et al., 2008). The hypothetical dimension is a probability relevant dimension that explains the psychological distance for an event that is more likely to happen compared to an event with remote possibilities of happening (Wakslak et al., 2006). The probability of an event's occurrence not only impacts the individual's perception regarding the event, but it also can have significant implications on the decision and the course of actions regarding this event (Todorov, Goren, & Trope, 2007). Dimensions such as time, place, people, and the probability of occurrence influence the psychological process of event interpretation. Therefore, according to CLT, an event will be at a greater psychological distance when it is farther into the future, occurs in remote locations, less likely to occur, or affects other people (Liberman, Trope, & Wakslak, 2007).

CTL explained that the detailed and physical presentation of the actual product, as opposed to being represented abstractly by a verbal brand name, directed consumers to have accurate judgment of the product (Krishna, 2012). Increased psychological distance increased the desirability perception of the system's ease of use and usefulness and increased adoption intention (Ho et al., 2015). When CLT was applied to evaluate customers' online reviews, results reflected that the increased distance and abstraction created more positive perception of the event and positive feedback (Huang, Burtch, Hong, & Polman, 2016). In a CLT study focused on understanding the psychology of password management, researchers found that manipulating the psychological distance, such as time, can positively influence the tradeoff between security and convenience to influence individuals to follow secure behavior (Tam, Glassman, & Vandenwauver, 2010).

A construal, in the context of information security is equivalent to a thereat context. CLT suggests that the concreteness or abstractness of a construal as experienced by the individual governs their behavioral choice. The key psychological constructs that capture these behavioral choices are desirability and feasibility. These constructs are similar to the PMT constructs of threat appraisal and coping appraisal. Liberman and Trope (1998), explained that the distinction between feasibility and desirability corresponds to the distinction between means and ends. Desirability refers to the outcome, ends, or goals, whereas feasibility considerations explain action alternatives to achieve the desired outcome or goals.

In this section, we outline the two new constructs based on CLT – threat un-desirability and coping feasibility. We compare and contrast these with existing conceptualization from PMT regarding threat appraisal and coping appraisal. We also present arguments of how these fit into the model and why they in turn influence behavioral choice. The application of CLT in the context of information security explains individuals' psychological processes that influence the perception of the un-desirability of a threat and the feasibility of the countermeasure in terms of personal psychological distance.

3.4.2 Threat Un-desirability

Threat un-desirability refers to the perception of the extent to which an individual will personally be affected by the threat. Consistent with CLT primes, abstract knowledge about an event directs individual's attention to the desirability of that event (Ho et al., 2015). In the context of information security, the abstractness or concreteness of knowledge regarding information threats can be perceived in terms of threat un-desirability. Therefore, it is relevant to re-conceptualize the threat appraisal from a personal un-desirability perspective (threat un-desirability). While the evaluation of threat un-desirability sounds similar to the PMT construct of threat appraisal, which is the personal perception regarding the severity of and vulnerability to a threat (Rogers, 1983), it differs in three ways, as shown in Table 5.

Table 5: Threat Appraisal Compared to Threat Un-Desirability

	Threat Appraisal	Threat un-Desirability
Definition	The individuals' assessment of their own safety if they follow a certain risky behavior (Floyd et al., 2000)	The extent to which an individual perceives the personal impact by the threat
Locus	Organization	Individual - Threat
Measuring what	Magnitude	Psychological distance
Process	Cognitive assessment	Affective assessment

As Table 5 shows, threat un-desirability differs from threat appraisal in three ways: locus, measures, and process. The original context of PMT refers to threat appraisal as the individuals' assessment of their own safety if they follow a certain behavior (Maddux & Rogers, 1983). However, the locus of threat appraisal in information security research is how well an individual understands organizational threat (Warkentin et al., 2016). The position of the threat was removed from a personal threat and became an organizational threat. Threat un-desirability refers to the extent to which an individual will perceive a personal impact by the threat. Therefore, threat un-desirability's locus is the individual.

Another difference between threat appraisal and threat un-desirability in the context of information security is the measure of threat impact. The appraisal of information security threats measures the magnitude of damage towards the organization (Sommestad et al., 2015). Threat un-desirability measures the perception of the threat based on psychological distance from the individual. For example, people find it less desirable to share private information on a government website because the perception of exposure to a personal threat is greater (Crossler, 2010). By contrast, violations against organizational information can be more desired if it leads to increased productivity (Siponen & Vance, 2010).

The third difference between threat appraisal and threat un-desirability is the basis of the process of threat by the individual. Threat appraisal is a process that influences the individual's cognition regarding a specific threat to motivate protection (Sommestad et al., 2015). However, as we argued earlier, despite the importance of cognition, behavioral drivers are affective. Threat un-desirability is the affective assessment of the threat that motivates behavioral choice.

Literature shows that the threat appraisal process is conceptualized through organizational threat. Threats to the security of organizational information are broadly construed to mean modification, destruction, theft, or lack of availability of organizational computing assets and services (Straub & Welke, 1998). That places abstractness to the threat and increases the psychological distance directing perception towards desirability (Krishna, 2012; Trope et al., 2007). Lack of information security knowledge presents abstract perception of security threats which may lead an employee to believe that security violations are less harmful (Vance et al., 2012). Literature supports that complex security measures, which increase psychological distance from the employee, may increase violations' desirability (D'Arcy et al., 2014). People find it less desirable to share private information on a public website because the appraisal of threat is greater (Crossler, 2010). However, the increase in productivity justifies violations against organizational information (Siponen & Vance, 2010). Therefore, consistent with CLT propositions of psychological distance, PMT construct threat appraisal can be reframed on a personal level in terms of threat un-desirability.

The appraisal of the threat is strongly related to protection motivation when the target of the threat is the person himself or herself but not someone else or the organization (Sommestad et al., 2015). Therefore, consistent with CLT, the concrete perception of a threat and its severity brings this threat to a closer psychological distance to the individual increasing threat un-desirability and increasing protection motivation. Threat assessment will shape employees' attitude towards compliance (Herath & Rao, 2009b; Warkentin et al., 2016). Individuals are more likely to follow protective behavior when the threat's damaging impact is severe (Vance et al., 2012; Workman et al., 2008). Information security literature supports that severity of the threat and its harmful impact significantly affect employees' concerns regarding security breaches (Chen et al., 2012; Herath & Rao, 2009b). In the information security domain, PMT has been used in contexts where the threat is rather abstract (Sommestad et al., 2015) and vulnerability is explained to be towards the organizational information systems rather than the individual (Johnston et al., 2015). Thus, employees may feel invulnerable to the threat. Abstract perception of threats increases the personal psychological distance to the threat directing the individual perception to the desirability of the threat.

Employees may rationalize violations when threat is abstract (Siponen & Vance, 2010). The personal understanding of the damaging details of the threat will bring threat to a closer psychological distance, which will increase threat un-desirability. Threat un-desirability is the personal assessment of the damaging impact of the threat. When threats are explained in more detail, threats become less desirable. Therefore, with the decreased desirability of the threat, employees' secure behavior can become a personal behavioral choice. As threats become less desirable by the employee, the more motivated the employee can be to follow protective behavior. Therefore, the following hypothesis is proposed:

H4: The greater the threat un-desirability, the higher the protection motivation.

3.4.3 Coping Feasibility

Coping feasibility refers to the process by which individuals evaluate the effectiveness of the available risk mitigating behavior. Individuals' attitude is influenced by their evaluation of the feasibility of the response (Warkentin et al., 2016). Feasibility consideration focuses on the level of difficulty regarding the action alternatives to achieve the desired outcome or goals. CLT research supports that the increased knowledge regarding how to apply a recommended action directs individuals' perception to feasibility of the action (Köhler et al., 2011). As knowledge explains the details and the features of the coping mechanism, intentions will be focused on the feasibility (Ho et al., 2015). Therefore, it is relevant to re-conceptualize the response appraisal from the feasibility perspective (response feasibility). The difference between coping appraisal and coping feasibility is shown in Table 6.

Table 6: Coping Appraisal Compared to Coping Feasibility

	Coping Appraisal	Coping Feasibility
Definition	The coping appraisal is the process by which individuals evaluate how effective, manageable, and feasible the available risk mitigating response can be (Ifinedo, 2012)	Coping feasibility refers to an individual's attitude towards the efficacy and difficulty of the individual action required to prevent / mitigate the threat
Locus	Task	Individual - Action
Measuring what	Effectiveness and Skill	Difficulty perception
Basis	Efficacy	Effort

As Table 6 shows, coping feasibility differs from coping appraisal in three ways: locus, measures, and process. The original intent of PMT posits that coping appraisal is the process by which individuals evaluate how effective, manageable, and feasible the available risk mitigating response can be (Ifinedo, 2012). The locus of coping appraisal in the context of information security is the task to be performed by the individual. Coping feasibility is concerned with the individual's perception of the ease (difficulty) in performing a successful mitigating action. Therefore, the locus of coping feasibility is the individual.

Another difference between coping appraisal and coping feasibility in the context of information security is what is being measured. Coping appraisal is concerned with the availability of a coping mechanism and the ability to perform what is required to avert the threat (Floyd et al., 2000). Coping feasibility is the process by which an individual's attitude towards a recommended secure behavior is based on the perception of the degree of difficulty to follow that behavior. This research argues in the model that the end user's perception of threat drives the behavior. Therefore, it is relevant to measure the individual’s perception of the desired secure behavior, or response efficacy, and the degree of difficulty to follow that behavior, or response difficulty.

Finally, the basis of the process of coping appraisal is the individuals’ belief in their ability to implement a certain prescribed coping mechanism. Coping appraisal basis are self-efficacy, response efficacy, and response cost (Boss et al., 2015). Coping feasibility is based on the individual’s perception of the adequacy of the mitigating action, response efficacy, and the associated efforts needed to implement successfully that available action, or response difficulty.

Researcher found that the individuals perception of the available response has the most significant influence on forming intentions and behavior (Sommestad et al., 2015). Individuals’ belief in their own abilities to perform what is required to avert the threat can influence intentions (Bulgurcu et al., 2010). The positive perception is enabled by employees’ relevant knowledge, competence and capability to implement preventative security measures (Ifinedo, 2012). Researchers have shown that the individual’s capacity to participate in an affordable threat mitigating action can positively influence intentions (Herath & Rao, 2009a; Sommestad et al., 2015). When organizations engage people to implement protective actions that they actually can take, they are more motivated for protection (Warkentin et al., 2016). Information security literature suggests the positive impact of the feasibility of response on employees’ intentions (Johnston et al., 2015; Warkentin et al., 2016). The literature suggests that when the desired response is clear and not abstract, protection motivation increases (Sommestad et al., 2015), and that is consistent with CLT, as details direct perception to feasibility (Ho et al., 2015).

Interestingly, researchers found that the increased complexity and difficulty of the desired protective response had a negative impact on protection motivation (D'Arcy et al., 2014). Hindrance to employees' productivity caused by security requirements is one of the reasons for employees to neglect the recommended behavior (Herath & Rao, 2009b). Employees may actually feel justified not to follow secure behavior if it is perceived to be convoluted and gets in the way of their productivity (Siponen & Vance, 2010). The increased cost of secure behavior can have a negative impact on protection motivation (Herath & Rao, 2009b). Research findings suggest that if the response is not feasible, employees may not follow it.

Coping feasibility is the personal assessment of response efficacy and the difficulty to follow that response. As researchers suggested, based on the original intents of PMT, as the coping feasibility increases, the protection motivation also increases. Furthermore, as the complexity of the coping mechanisms decreases, the protection motivation increases. Therefore, we argue that the increased coping feasibility can positively impact the individual's motivation to follow a secure behavior. Therefore, the following hypothesis is proposed:

H5: The greater the coping feasibility, the higher the protection motivation.

3.5 Secure Behavior

The primary focus of PMT is to predict intentions toward protection motivation (Maddux & Rogers, 1983). Researchers argued that PMT was successfully extended to predict behavior and not just the motivation because there is a link to actual behavior (Floyd et al., 2000). The goal is not just to motivate employees but also to change their behavior. PMT can be applied to measure actual behavior (Crossler et al., 2013).

Protection motivation, similar to other types of motivation, reflects the level of desire and willingness that directs behavior (Floyd et al., 2000). Researchers argued that protection motivation is the strongest predictor of behavioral change (Boss et al., 2015). Thus, although the independent variable in this research is protection motivation, this independent variable can be used as a proxy to predict the actual secure behavior.

Prior research efforts demonstrated a clear linkage between intention and actual behavior (Johnston et al., 2015). This approach is supported by numerous empirical research studies because the intention is viewed to be an indication of a precondition to a behavioral act (Siponen et al., 2014). Compliance intention is an antecedent and a strong predictor of actual behavior (Sommestad & Hallberg, 2013).

3.6 Chapter Summary

The theoretical development presented in this chapter builds on the gaps and findings synthesized from the reviewed literature. The model conceptualizes organizational knowledge mechanisms, training and policy, across three dimensions: breadth, depth, and finesse to explain how any threat is perceived by the end-user. The proposed model is threat agnostic. This allows the research to be generalizable across different known threats as well as new threats that may emerge. Knowledge breadth connects wide range of threats that the organization may face to increase employees' ability to distinguish between threats that users otherwise may think irrelevant. Knowledge depth presents the completeness of knowledge in order for employees to know how to perform any activity. Finesse is the ability to apply innovativeness through collaboration and brainstorming to create feasible approaches to enhance performance and increase the feasibility of secure behaviors.

The model follows PMT to explain the psychological process of protection motivation that is influenced by the personal perception of threat and the available coping mechanisms. In the context of information security, PMT showed inconsistent results due to lack of personalization as threats toward organizations instead of the person did not accurately present the intent of PMT. CLT provides a means to measure the psychological constructs of PMT from an individual's perspective, i.e., personalizing them. CLT explains that abstract knowledge about an event directs individual's perception to the desirability of that event, whereas detailed knowledge directs the perception towards feasibility. Therefore, it is relevant to re-conceptualize the PMT constructs (threat appraisal and coping appraisal) from a personal perspective as threat un-desirability and coping feasibility. Threat un-desirability focuses on the individual's perception of a personal impact by the threat. Consistent with CLT, when threats are explained in more details, threats become less desirable and with the decreased desirability of the threat, employees' secure behavior can become a personal behavioral choice. Similarly, coping feasibility focuses the personal perception on the level of difficulty regarding the action alternatives to achieve the desired secure behavior. The increased feasibility of the mitigating action can positively impact the individual's motivation to follow a secure behavior. PMT was successfully extended to predict behavior and not just the motivation. Literature supports that protection motivation is an antecedent and a strong predictor of actual behavior. Therefore, the presented dependent variable in this model, protection motivation, should be capable of predicting secure behavior.

CHAPTER 4 – RESEARCH DESIGN

This chapter presents the quantitative research design used to test the research model and to examine the relationships between variables in order to answer the research questions. The methodological approach proposed in this chapter followed a two-study approach to answer both research questions:

Q1: What are the key psychological processes that influence employees' secure behavior when dealing with an information security threat?

Q2: How do organizational knowledge mechanisms such as SETA programs and policies influence key psychological processes of threat perception?

Study one is an experiment designed to answer the first research question. In many research studies, experimental models are used when a convenience sample is possible with naturally formed groups such as students in a classroom (Creswell, 2014). Study two evaluates the entire research model, thus answering both research questions. Study two employs a quantitative survey design. The data is collected online from a sample of full-time working professionals. The survey assesses the relationships between the input constructs (knowledge dimensions), process constructs (threat un-desirability and coping feasibility), and the output construct (protection motivation). The proposed approach is consistent with recommendations from the marketing and information systems literature.

The following sections will explain each of the two studies. The sections will address the design, constructs involved, samples used, procedures, and data collection methods. The concluding section will summarize studies conducted.

4.1 Study One

The first research question aims to understand the key psychological processes of threat perception. To answer this question, the focus was on a subset of the research model. The entire research model was investigated in study two. Study one research model is shown in Figure 4.

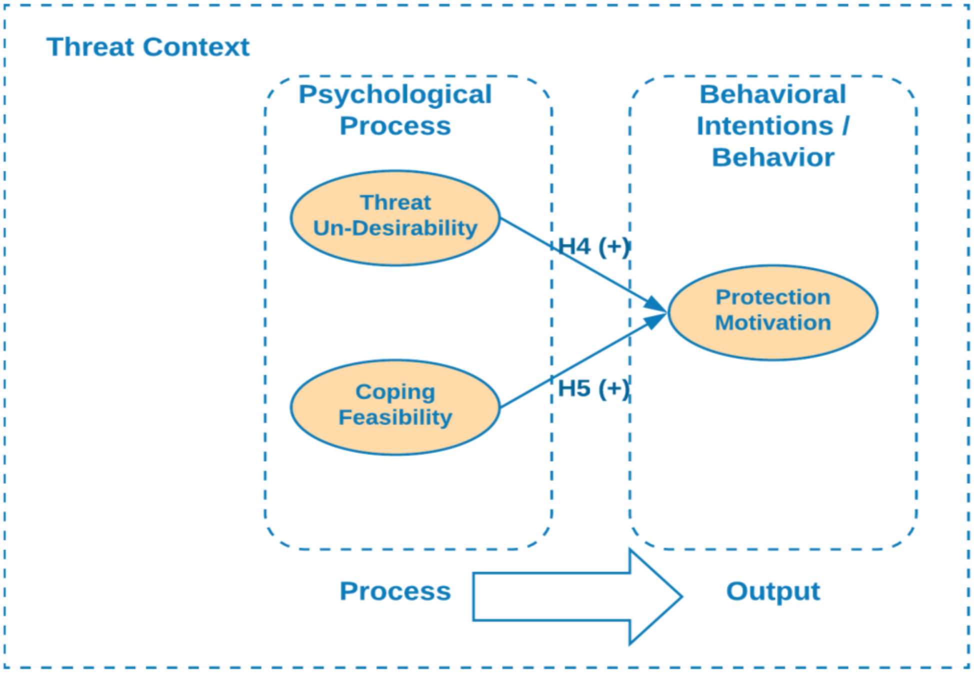

Figure 4. Study one model diagram

Study one measures how the concreteness or abstractness of a threat context impacts the participants' affective perception of that threat's un-desirability and coping feasibility. Therefore, in study one, a known threat context is manipulated and presented to participants with either concreteness or in a high level of abstraction. This scenario manipulation allows the researchers to measure the impact of the key constructs of the psychological process, threat un-desirability and coping feasibility, on protection motivation.

4.1.1 Research Method

To empirically validate the manipulation checks for these key psychological processes, this study applies a valid and operationalizable scenario-based, experimental research design. The intent of the experimental design is to test the impact of a treatment on the outcome (Creswell, 2014). In study one, the treatment is a scenario-based manipulation of the degree of abstractness or concreteness of a known threat context to measuring the impact on protection motivation. Using a scenario-based experiment allows the researcher to establish a reliable and valid measure for behavioral intention as it relates to the various factors found in the scenario (Willison, Warkentin, & Johnston, 2018). The use of experimental methods offer a high internal validity and allows for statistical controls (S. Gupta, 2006). The direct comparison of effects, while controlling other factors that might offer competing explanations, as well as the replications of the phenomenon provide high internal validity (Poole & DeSanctis, 2004). However, cross sectional studies do not account for maturation or history of participants or threats therefore they are limited in longitudinal generalization.

The experiment applies a scenario-based survey to validate empirically the instrument to measure the impact of these manipulations on protection motivation. Using a scenario-based analysis has been established and applied to IS research (Willison et al., 2018). This experiment is designed based on previous literature recommendations

(Campbell & Stanley, 1963, p. 50). In this design, the experimental control is achieved or enhanced by entering all groups into all manipulations.

4.1.2 Sample

The selected sample frame used for this experiment was undergraduate students enrolled in various business programs from a university in southeast region of the United States of America. This sample frame is appropriate because business students represent a sample of information systems end users who have valuable information that should be protected. Information systems literature shows that the use of students in information systems research is a common practice (Chatterjee et al., 2015). In the specific context of information security, Warkentin et al. (2016), supported the use of students as a reliable sampling frame for two reasons. First, students are members of an organization that requires information security compliance. Also, students are individuals with valuable informational assets, and therefore, they are subject to protection motivation factors as any system user. Therefore, the university business students present an adequate and relevant sample to evaluate factors impacting the perception of threat un-desirability and coping feasibility.

Participants were invited to participate in the experiment on a voluntary basis. All participating students received course credit. As this study focused on the psychological perception of knowledge workers, end-users, students majoring in Information Systems or Information Security were not included in the sample, as these students may not represent the typical end users. Also, they may represent perceptions influenced by prior experiences with security breaches. Some researchers addressed the positive relationship between prior experiences with security incidents and protection motivation (Boss et al., 2015; D. Lee et al., 2008).

The determination of sample size impacts the power analysis (Hair, Black, Babin, & Anderson, 2010, p. 174). As explained in Creswell (2014, p. 169), for experimental research, researchers use power analysis to identify the appropriate sample size for the groups. Researchers set values for three factors involved in the calculations of the sample size (alpha = 0.05, power = 0.80, and effect size = 0.5). As shown in the sample size table, Cohen (1988, p. 54), the appropriate sample size according to these three values is 50 participants for each group. This is also consistent with Hair, Black, Babin, Anderson, and Tatham (1998), as they stated a rule of thumb to require at least sample of 50 to maintain power at 0.80. G*Power software was also used to calculate the needed sample size. The calculated sample size by the software was consistent with the literature recommendation. Therefore, our target sample size for each group was 65 participants to account for unusable responses.

4.1.3 Experimental Procedure Manipulation

Following the Campbell and Stanley (1963) design, the experiment was applied in a randomized manner, as illustrated in Figure 5.

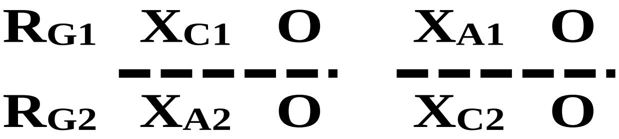

Figure 5. Experiment design diagram

The design contains three classifications: R_G is the random group, X is the manipulation, and O is the observation. Each treatment occurred once (X_C denotes the manipulations based on a concrete scenario, and X_A denotes the manipulations based on an abstract scenario). The subscript numbers in the diagram represents whether group 1 or group 2.

Students were randomly split into two groups, R_{G1} and R_{G2} as denoted in the diagram in Figure 5, to enhance external validity. Creswell (2014, p. 158) recommended randomization to increase the ability to generalize to a population. For the random group assignments, the randomization feature in Qualtrics Research Suite software was applied. Qualtrics software allows the researcher to evenly and randomly split participants into two groups based on a specified branching condition. In this experiment, the branching condition was either group 1 or group 2. This option automatically assigned each student randomly to be placed in one of the two groups and see only the part of the survey assigned to that group.

Each group received a one pair of scenarios (an abstract scenario and a concrete scenario) for a specific security threat context to work with. All participants in group 1 received the concrete version of scenario 1 (X_{c1}), while at the same time, all participants in group 2 received the abstract version of scenario 2 (X_{A2}). The scenarios were presented as animated short videos to both groups. The use of animation allows more control over the time needed to understand the scenarios. After watching the animated videos, students recorded their observations. For the observations, students were given scales that measured their perception of threat un-desirability and coping feasibility. When all scenario observations were recorded for both groups, the same process was repeated; however, group 1 received the abstract version of scenario 1 (X_{A1}) while group 2 received the concrete version of scenario 2 (X_{C2}).

It is argued here that the concrete description of a scenario, according to CLT, will construe the threat on a closer psychological distance from the participant directing their perception to the coping feasibility and increasing threat un-desirability. Also, the abstract scenario will construe the threat on a high psychological distance that will decrease the perception of threat un-desirability and reduce the perception of coping feasibility. The psychological distance was manipulated across the following distance dimensions:

- Temporal was measured by past, current, or future
- Spatial was measured by a nearby location compared to somewhere else
- Social was measured by events happening to self, known people, or random people
- Hypothetical was measured by true situations or imaginary activities

By manipulating the degree of abstractness or concreteness, the individual’s protection motivation will be impacted through threat un-desirability and coping feasibility. Hence, we developed the following hypotheses, as explained in the previous chapter and presented in the model, regarding threat un-desirability and coping feasibility:

H4: The greater the threat un-desirability, the higher the protection motivation

H5: The greater the coping feasibility, the higher the protection motivation.

To increase the contextual relevance, as explained by Siponen and Vance (2014), the scenarios clearly described the participant’s setting, environment, and the event that the participant was thinking about and had worked with. Each participant was asked to watch the scenarios and then respond to an online scenario-based survey instrument. The instrument measured threat un-desirability and coping feasibility perception among participants. See Appendix B for complete details regarding both scenarios, including the concrete and abstract written versions and the manipulation checks. The full instrument used for study one is included in Appendix C.

4.1.4 Measurements

As explained in the previous chapter, threat un-desirability refers to the extent to which an individual will perceive a personal impact by the threat. This was measured by the individual's psychological distance from a specific threat context. The experiment manipulated all four dimensions of psychological distance based on CLT. On the other hand, coping feasibility is concerned with the individual's attitude towards the mitigating action and the perception of the ease or difficulty in performing that threat mitigating action. This was measured by the individual's perception of response efficacy and difficulty. The experiment was used to manipulate participant's perception of the ease or difficulty to perform the desired coping mechanism. The dependent variable was protection motivation.

The scenarios described above were presented to the participants to measure their perceptions of threat un-desirability. After dealing with each threat scenario, participants were asked to rate their perceptions that reflected their own psychological distance from this threat context. Table 7 includes the psychological distance rating.

Table 7: Psychological Distance Rating

I believe that the risk from the threat is		
Distant/Future impact	1-7 scale	Imminent impact
General/Generic	1-7 scale	Personal
Made-up/Hypothetical	1-7 scale	Real
Far away/Somewhere else	1-7 scale	Close/Here

Coping feasibility was measured by evaluating the participants' perception of response efficacy and response difficulty. The participants' perception of coping feasibility was manipulated by the threat scenarios described above. Coping feasibility is a higher order construct that was measured by two formative constructs, response efficacy and response difficulty. The scale that measured response difficulty was adopted from S. Gupta (2006) (α = 0.946) and the scale that measured response efficacy was adopted from Workman et al. (2008) (α = 0.85). The instruments adopted were slightly modified to better match the specific context of this research. On a scale from 1-7, where 1 is strongly disagree and 7 is strongly agree, participants were asked to rate their own agreement with the coping feasibility questions. Table 8 shows the modified questions used in this research based on the original instruments by S. Gupta (2006) and Workman et al. (2008).

Table 8: Coping Feasibility Instrument

Coping feasibility
Response Difficulty from S. Gupta (2006) α = 0.946
Modified Instrument
• Protecting myself from this threat complicates my job tasks • Protecting myself from this threat will make my current job mentally demanding

• Protecting myself from this threat requires a lot of thought and problem-solving in my current job
Response Efficacy from Workman et al. (2008) (α = 0.85)
Modified Instrument
• Solutions available to keep my organization’s information / information systems safe from the threat are successful • The available measures that I can take to protect my organization’s information / information systems from the threat are effective • The preventive measures available to me to stop the threat are adequate

Finally, to measure protection motivation, the items below were adopted from Posey et al. (2015) with α = 0.64. On a scale from 1-7 where 1 is strongly disagree and 7 is strongly agree, participants were asked how motivated they are to take immediate action by rating the following:

1. I will protect myself from this specific threat
2. I will engage in activities to protect myself from this specific threat
3. I will prevent this specific security threat from being successful

4.1.5 Process and Statistical Control

It is important to identify factors that may interfere with outcomes and provide false positives. Controls are introduced to eliminate any external influence. Controlling for factors that may interfere with the outcome is critical so that participation in one group or the other will not impact the outcome (Creswell, 2014). Controlling for factors that might offer competing external explanations leads to a clearer analysis of the impact of psychological manipulation on the output behavior, which in this case was protection motivation. Through the use of experimental controls, it is possible to access perception and the impacts on protection motivation without the confounding factors present in real settings.

In this study we statistically controlled for the demographic of the sample such as gender, age, and computer experience. These controls are commonly used in information security behavioral research (Boss et al., 2015; D'Arcy et al., 2009; Herath & Rao, 2009b). We also proposed to statistically control for risk appetite. Risk appetite or risk propensity is defined as an individual’s tendency to take or avoid riskier decisions (Sitkin & Weingart, 1995). Therefore, we statistically controlled for participants’ risk propensity. The five-item scale (α = .86) from research by Sitkin and Weingart (1995) was used to measure risk propensity. The five-item scale is shown in Appendix A.

As part of study one, prior to conducting the survey, an expert panel comprising of four experts in research design and instrument development reviewed each scenario to ensure realistic scenario contents and validate the presence of all psychological distance dimensions. Following the panel’s recommendations, minor changes were applied to the survey, such as word modifications.

4.1.6 Analysis

To assess the consistency and reliability of the scale measuring threat un-desirability, a paired t-test method was used. Paired t-tests are used to determine the difference in mean responses among groups (Hendrickson, Massey, & Cronan, 1993). Also, to further increase the external validity of the manipulations, the experiment used concrete and abstract versions of two threat scenarios to present a more realistic and generalizable assessment of psychological process output that would be applicable in any professional organization. In the meantime, the partial least squares (PLS) statistical analysis was performed to measure the relationship between independent variables (threat un-desirability and coping feasibility) and the dependent variable protection motivation. This approach has been established in business research (Hair, Ringle, & Sarstedt, 2011).

Descriptive statistics such as age, gender, degree level, major, and computer use was provided to explain the structure of the participants. Manipulation checks were designed to measure the variability in perception based on the psychological distance changes. To see the difference in perceptions, the measurement and the structural components of the model used for study one were tested using paired t-test and a path analysis modeling SEM technique. The component-based partial least squares (PLS) approach was used to evaluate the model proposed in study one.

4.2 Study Two

The objective of study two is to test the entire research model. The second research question aims to understand the way organizational knowledge mechanisms such as SETA programs and policy influence key psychological processes of threat perception. To answer this question, study two evaluated the entire research model as shown in Figure 6.

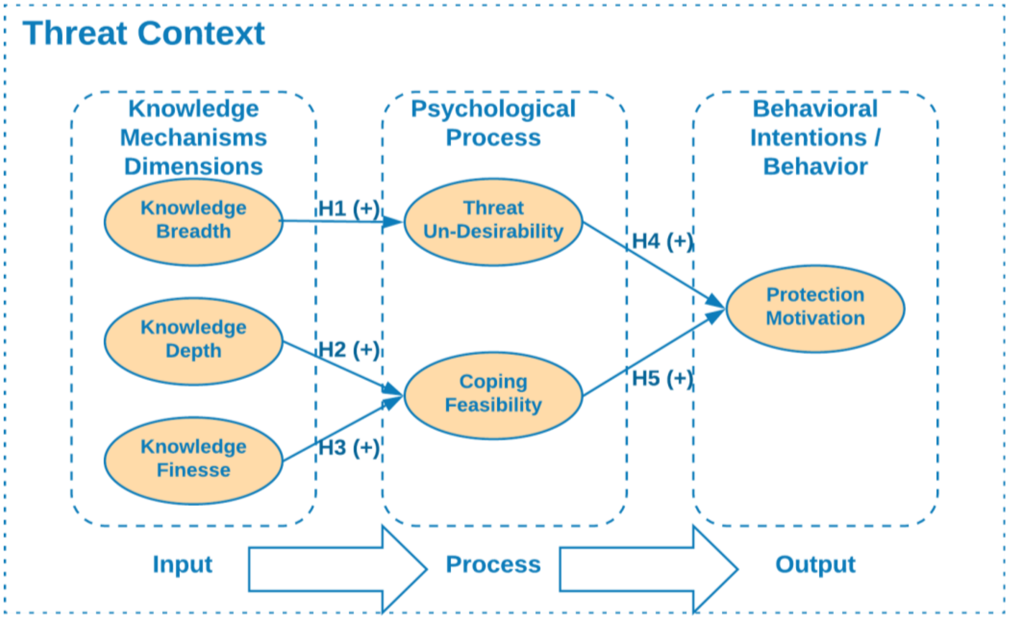

Figure 6. Research model

The model represents the impact of knowledge dimensions (breadth, depth, and finesse) on protection motivation, while fully mediated by the individual’s affective perception of threat un-desirability and coping feasibility. The model created, in a form of input-process-output, is suitable for analysis based on the hypothesized relationships. The following hypotheses that were explained in the previous chapter was tested:

H1: The greater the breadth of knowledge in knowledge mechanisms, the greater the un-desirability of threat by end-users.

H2: The greater the depth of knowledge in knowledge mechanisms, the higher the coping feasibility.

H3: The greater the finesse, the higher the coping feasibility.

H4: The greater the threat un-desirability, the higher the protection motivation.

H5: The greater the coping feasibility, the higher the protection motivation.

4.2. 1 Research Methods

Study two implemented a web-based survey design for data collection. Survey design enables a generalizable quantitative description of the targeted population's attitudes (Creswell, 2014). Online surveys provide several advantages, such as economy, speed of return, error checking, a computer assisted instrument, time to provide thoughtful answers, anonymity, and a far reaching geographical distribution (Fowler Jr, 2013). Web-based surveys have been previously used in similar research to enable data collection from a large sample of business professionals (Crossler, 2010).

A holistic approach, considering critical aspects for survey process, was followed as explained in the literature. It is critical to consider the basic steps in survey process, such as defined objectives, population and sample frame, data collection strategy, time, budget, resources constraints, the questionnaire creation, data collection, and data analysis (Sue & Ritter, 2007). The survey is cross-sectional, with the data collected at one point of time from business professionals. Participants were asked to complete the online questionnaire while imagining themselves facing a context of a real information security threat. To reduce problems with the reliability and validity of questionnaire, whenever possible, we adopted the items from previously validated studies. Using validated and tested questions improves the reliability of results (Straub, 1989).

4.2.2. Sample

A key requirement for a high quality sample is representativeness of the population of interest (Hair et al., 2010, p. 523). Selecting the appropriate representative sample provides the ability to generalize to the population (Creswell, 2014, p. 158). The survey was sent out to a diverse sample of business professionals for data collection. As this study aims to understand end-user psychological perception regarding information security threats, the data were collected from a random sample of full-time business professionals who use information systems for their daily jobs. The sample did not include unemployed, retired professionals, or labor workers who do not use enterprise information systems daily to accomplish their job related tasks. Because this sample may not reflect the end user's psychological perception regarding information security threats. Also, IT professionals were excluded from the sample, as their prior experiences may influence their motivation to protect information (Boss et al., 2015; D. Lee et al., 2008).

Based on the set of factors explained by Hair et al. (2010, p. 644), the minimum sample size used for this study should be 150 participants. However, to account for the missing data and unusable responses, more than 200 responses were collected to ensure an adequate sample size that can be used for the data analysis process. The sample included males, females, full-time employees, senior experienced professionals, and junior professionals in organizations within the Unites States. The data that was collected targeted an evenly distributed sample of employees in terms of age, gender, employment type, and work location. Such heterogeneity of the data sample supports representativeness for the targeted population and reduces potential bias arising from a limited employee representation in the data collection process.

4.2.3 Measurements

Validated measuring scales were used in this study. The survey adapted items used by Zhou and Li (2012) to measure knowledge breadth and knowledge depth. The survey included three questions for items measuring knowledge breadth ($\alpha = 0.84$) and three questions for items measuring knowledge depth ($\alpha = 0.78$). Also, the survey included adapt items used by Munro et al. (1997) to measure finesse. A slight modification of the instrument was applied to better align the instrument to the specific context of information security. Table 9 shows the modified instrument used in this research to measure knowledge dimensions.

Table 9: Knowledge Dimensions Items

Knowledge Breadth ($\alpha = 0.84$) by Zhou and Li (2012)
Modified Instrument
My organization's information security policies and training programs help me: • Acquire diversified and wide-ranging security knowledge • Accumulate knowledge of multiple security threats • Gain variety of technical knowledge about information security
Knowledge Depth ($\alpha = 0.78$) by Zhou and Li (2012)
Modified Instrument
My organization's information security policies and training programs give me: • Thorough understanding and experience of specific security threats • In-depth knowledge of the key information security threats that we face • Technical skills to mitigate specific threats targeting my domain of work
Finesse ($\alpha = 0.78$) by Zhou and Li (2012)
Modified Instrument
My organization's information security policies and training programs allow me to: • Leads to new solutions to replace older threat mitigating actions
Knowledge Finesse Munro et al. (1997)
Modified Instrument
My organization's information security policies and training programs allow me to: • Apply my experience innovatively to face new and different security threats • Be creative to solve security problems at work

The same items used in study one were also used in this study to measure threat undesirability and coping feasibility constructs. Finally, protection motivation, as explained earlier, was be measured by three items. Please refer to Appendix A for full details regarding items measuring protection motivation.

All constructs were measured formatively with multiple items on a seven-point Likert scales. Table 10 presents a summary of all used constructs in study two. The full instrument used to measure study two constructs is included in Appendix C.

Table 10: Constructs Summary

Construct	α	Cited
Knowledge Breadth	0.84	Zhou and Li (2012)
Knowledge Depth	0.78	Zhou and Li (2012)
Knowledge Finesse	NA	Munro et al. (1997)
Threat un-Desirability	NA	Authors
Coping Feasibility: Response Difficulty	0.946	(S. Gupta, 2006)
Coping Feasibility: Response Efficacy	0.85	Workman et al. (2008)
Protection Motivation	0.64	Posey et al. (2015)
Protection Motivation	0.983	Johnston et al. (2018)
Risk Propensity (statistical control)	0.86	Sitkin and Weingart (1995)

4.2.4 Process and Statistical Controls

Data were collected using online survey. The online survey was designed and completed using Qualtrics Research Suite software. A professional company was contracted for the recruitment of participants and the administration of the online survey. The benefits of using professional survey provider was extensively discussed in the literature (Creswell, 2014; Sue & Ritter, 2007). Similar to study one, study two statistically controlled for the demographic of the sample, such as gender, age, computer experience. These controls are commonly used in information security behavioral research (Boss et al., 2015; D'Arcy et al., 2009; Herath & Rao, 2009b). This study also controlled for risk appetite, as it impacts individuals' tendency to make risker decisions (Sitkin & Weingart, 1995). Therefore, risk propensity was measured in this study.

Participants were asked to imagine themselves facing a particular known information security threat and imagine their own actions while completing the survey questions. The survey was based on the items explained earlier. Based on the analysis of all responses, the incomplete, missing, or unreliable responses were discarded.

4.2.5 Hypothesis and Data Analysis

Knowledge breadth represents the broad understanding of wide range of diverse information security threats. Three reflective indicator items measured knowledge breadth. This study proposes a positive impact of knowledge breadth on the un-desirability of threat by end-users. Knowledge depth represents complete understanding of steps needed to address any threat in a specific context. Three reflective indicator items measured knowledge depth. This study proposes a positive impact of knowledge depth on the coping feasibility. Finesse is the ability to creativeness and innovativeness to the available course of action. Five reflective indicator items measured finesse. This study proposes a positive impact of finesse on the coping feasibility.

The measurement and the structural components of the entire model was tested using SEM technique. SEM is an appropriate statistical approach to examine the relationships of the entire theoretical model (Hair et al., 2010). While SEM is a general term encompassing a variety of statistical models, the theoretical model proposed in this study will be tested using partial least squares structural equation modeling (PLS-SEM). The PLS-SEM is the preferred method when the objective is prediction of structural relationships (Hair et al., 2011). PLS-SEM is increasingly applied approach to examine structural equation (Hair, Sarstedt, Ringle, & Mena, 2012). The use of PLS-SEM is an appropriate approach as it has the ability to handle sample size issues better. It also can handle complex theoretical models, such as the proposed model in this study and provide accurate estimates. Smart-PLS software package was used for the data analysis.

The demographic characteristics of the participants were reported. Descriptive statistics of the participants, such as age, gender, education level, work experience, work division or department, and computer experience was provided to explain the structure of the participants. The five item scale for risk propensity, adapted from Sitkin and Weingart (1995), were also used as a control variable.

As recommended by Hair et al. (2011), construct reliability and validity must be considered to guarantee an accurate measurement of the constructs used. Accordingly, the quality of the constructs was assessed by examining the factor loading for internal validity and Cronbach’s alpha for reliability. Factors show small Cronbach alpha indicating low correlation between items. The calculated Cronbach’s Alpha and Composite Reliability should show scale reliability and internal consistency of constructs in the model with all values above 0.7. Reliability is the measure of how highly interrelated the items or indicators that measure the construct with each other to reflect that all indicators actually measure the same thing. High reliability is associated with low measurement error (Hair et al., 2010).

CHAPTER 5 – DATA ANALYSIS

This chapter focuses on the data analysis conducted to empirically validate the relationships between variables in the proposed model. First, we discuss study one and associated statistical controls, as well as constructs validity and reliability. The study focused on the subset of the entire model that addresses the impact of the perception of threat un-desirability and coping feasibility on protection motivation. Study one also includes comparative analysis to compare the traditional PMT model to the model presented by this research. Following study one data analysis, we will discuss study two and evaluate the results to test each hypothesis. Finally, we provide findings and results for each of the hypotheses tested. The following sections below explain the details of the data analysis process.

5.1 Study One Data Analysis

Study one is an experiment designed to measure how concreteness or abstractness of a threat context influences the participants' affective perception of that threat's un-desirability and coping feasibility. In this experiment, a certain threat context was manipulated and presented to participants with either concreteness or in a high level of abstraction.

5.1.1 Sample Frame and Used Sample

The selected sample frame for study one was undergraduate students enrolled in various business major programs from a university in southeast region of the United

States of America. Students were invited to voluntarily participate in the study. Instructors of several business classes announced to their students that they would receive an anonymous web link to the survey and encouraged them to participate.

The survey link was shared with 457 students enrolled in various business classes. From the total students received the link, 314 students participated in the survey. The response rate was 68.7%. Survey responses were inspected for completeness and accuracy. Consequently, 36 incomplete responses were removed. An additional 16 responses from computer science and information systems students were removed. The total number of responses used in the data analysis was 262 responses, 57.3% of the sample frame.

5.1.2 Descriptive Statistics

The 262 responses utilized included 49.2% females, 50.0% males, and 0.8% preferred not to disclose. For the majority of respondents, 95.0%, were between 18 and 30 years old. Students from all four academic classes participated in the survey, including 8.8% freshmen, 32.4% sophomores, 27.5% juniors, and 31.3% seniors. The 262 participants were split evenly and randomly into two groups using Qualtrics, the online research software. Each group included 131 participants and had a balanced demographic distribution. Both groups one and two each received one pair of scenarios (an abstract scenario and a concrete scenario) for two specific threat contexts to work with.

This study considered several control factors that could influence participants' protection motivation such as participants' age, gender, academic class, major, computer experience, and risk appetite. These control variables were included in the data analysis to account for the influence of these variables on protection motivation. An independent sample t-test was conducted to compare means of all of the statistical control variables, gender, age, academic class, academic major, computer experience, and risk appetite. The analysis of the results of the independent sample t-test regarding all experimental control variables showed no significance in the difference between the two groups for all statistical control variables. Table 11 shows the detailed results of the independent sample t-test for all the experimental/statistical controls.

Table 11: Groups Independent Sample t-test for all Experimental Statistical Controls

Group Statistics				
Controls	Group 1 Mean (SD)	Group 2 Mean (SD)	Mean Difference	Sig. (2-tailed)
Computer Experience	3.01 (.72)	3.07(.81)	-.06	.52
Risk Appetite	2.87(.96)	2.94 (1.06)	-.07	.58
Gender	1.54 (.54)	1.48 (.50)	.057	.377
Age	2.35 (.67)	2.33 (.66)	.023	.780
Class	2.82 (.98)	2.81 (.98)	.008	.950
Major	6.21 (1.93)	6.47 (1.83)	-.260	.265

*$p < 0.05$;

As the results show in Table 11, there was no significant difference between groups. The automated randomization process for groups was successful, and the analysis concluded that both groups were equal. Consequently, these statistical controls were dropped from any further analysis of results in study one.

5.1.3 Construct Validity and Reliability

The next step was performed to test the construct validity and reliability of the key measures used in this study – threat un-desirability, coping feasibility, and protection motivation. The proposed measures for threat un-desirability are the four dimensions of the psychological distance forming the threat un-desirability higher order construct. The four dimensions are temporal (TUDPD-Temp), social (TUDPD-Soci), spatial (TUDPD-Spat), and hypothetical (TUDPD-Hypo). Three items labeled TUDPD-Temp1, TUDPD-Temp2, and TUDPD-Temp3 measured the temporal dimension. The social dimension was measure by three items labeled TUDPD-Soci1, TUDPD-Soci2, and TUDPD-Soci3. The spatial dimension was measure by three items labeled TUDPD-Spat1, TUDPD-Spat2, and TUDPD-Spat3. The hypothetical dimension was measure by three items labeled TUDPD-Hypo1, TUDPD-Hypo2, and TUDPD-Hypo3. The measures for higher order coping feasibility construct are the two formative constructs, response difficulty (RD) and response efficacy (RE). The response difficulty construct was measured by three items (RD1, RD2, RD3) and the response efficacy construct was measured by three items (RE1, RE2, RE3). Finally, the protection motivation construct was measured by five items (PM1, PM2, PM3, PM4, PM5).

A confirmatory factor analysis (CFA) was performed to confirm first order constructs. Software used was Smart-PLS version 3 (Ringle, 2015). The procedures used were partial least squares (PLS) and PLS bootstrapping (5000 runs). The outer loadings were analyzed for all items measuring the proposed constructs. Table 12 shows the outer loadings results for all items.

Table 12: CFA all Items loadings with P-Values

Items	Outer Loadings	T Statistics (|O/STDEV|)	P Values
PM1 <- PM	0.82*	44.12	0.00
PM2 <- PM	0.86*	51.88	0.00
PM3 <- PM	0.87*	69.17	0.00

PM4 <- PM	0.44*	8.20	0.00
PM5 <- PM	0.85*	53.46	0.00
RD1 <- RD	0.93*	1.92	0.03
RD2 <- RD	0.94*	1.92	0.03
RD3 <- RD	0.89*	1.93	0.03
RE1 <- RE	0.90*	24.16	0.00
RE2 <- RE	0.93*	24.62	0.00
RE3 <- RE	0.88*	22.42	0.00
TUDPDHypo1 <- Hypo	0.87*	60.34	0.00
TUDPDHypo2 <- Hypo	0.86*	61.87	0.00
TUDPDHypo3 <- Hypo	0.01	0.13	0.45
TUDPDSoci1 <- Soci	0.82*	49.41	0.00
TUDPDSoci2 <- Soci	0.74*	23.55	0.00
TUDPDSoci3 <- Soci	0.88*	75.25	0.00
TUDPDSpat1 <- Spat	0.12	1.42	0.08
TUDPDSpat2 <- Spat	0.88*	86.89	0.00
TUDPDSpat3 <- Spat	0.86*	59.25	0.00
TUDPDTemp1 <- Temp	0.82*	38.11	0.00
TUDPDTemp2 <- Temp	0.82*	44.76	0.00
TUDPDTemp3 <- Temp	0.81*	42.91	0.00

*$p < 0.05$

As shown in table 12, most of the proposed items were significant and showed strong and high loading scores. However, items TUDPD_Hypo3 and TUDPD_Spat1 showed low loadings at 0.01 and 0.12 respectively. Also, these two items were statistically not significant, with P-value scores higher than 0.05. Based on the analysis of the loading results, items TUDPD_Hypo3 and TUDPD_Spat1 were removed. Removing these items was reasonable to improve the overall model scores.

Following the analysis of outer loadings, using the remaining items, each construct reliability and validity was tested. The values for composite reliability, the

Cronbach's Alpha, the average variance extracted (AVE), and discriminant validity were checked to evaluate constructs reliability and validity. Table 13 shows the values for Cronbach's Alpha, AVE, and composite reliability. The discriminant validity test was performed, and results were included in Table 13 as well. The results of the discriminant validity, the diagonal values (in boldface) in the table, were greater than any of the internal factors correlations (or correlations of the constructs) for all constructs. All AVE and composite reliability values are indications of conversion validity. Also, all Cronbach's Alpha values are high. Although the Cronbach's Alpha score for the construct labeled "Hypo", representing the hypothetical dimension of the psychological distance to threat un-desirability, was slightly lower than 0.7 at 0.68. All other scores for this construct such as loadings, composite reliability, AVE, and discriminant validity are high.

Table 13: Constructs Reliability and Discriminant Validity

	Cronbach's Alpha	Composite Reliability	AVE	PM	RD	RE	Hypo	Soci	Spat	Temp
PM	0.83	0.89	0.62	**0.79**						
RD	0.91	0.94	0.85	-0.05	**0.92**					
RE	0.89	0.93	0.81	0.40	-0.12	**0.90**				
Hypo	0.68	0.86	0.75	0.48	-0.10	0.30	**0.87**			
Soci	0.75	0.86	0.66	0.40	0.06	0.17	0.62	**0.81**		
Spat	0.70	0.87	0.77	0.47	0.02	0.16	0.64	0.73	**0.88**	
Temp	0.75	0.86	0.66	0.50	-0.01	0.24	0.71	0.69	0.73	**0.82**

The Heterotrait-Monotrait ratio (HTMT) discriminant validity test was performed. Table 14 displays the summary of the HTMT test results. The test results show that the values associated with PM, RD, and RE constructs are below the HTMT critical value and the discriminant validity was established. However, as expected with the psychological distance constructs, some of the values were slightly above the HTMT critical value. Because these are formative constructs and are expected to have cross loadings, we performed the HTMT test on the latent constructs of the model, PM, CF, and TuD. Table 15 shows the summary for the HTMT test results on the model's constructs. All values in the table were below the HTMT critical value. That confirms discriminant validity among the model's constructs.

Table 14: Summary of the HTMT Discriminant Validity Test

	PM	RD	RE	Hypo	Soci	Spat
RD	0.08					
RE	0.47	0.13				
Hypo	0.64	0.13	0.39			
Soci	0.50	0.09	0.20	0.87		
Spat	0.61	0.12	0.20	0.90	1.00	
Temp	0.65	0.09	0.29	1.00	0.90	1.00

Table 15: Model Constructs' HTMT Discriminant Validity

	CF	PM
PM	0.39	
TuD	0.27	0.61

We also examined the Inner VIF for all items. All items VIF scores were less than the cutoff value of 5. Next, we examined the contribution of each component in the measurement diagram. Broadly, all of TuD components contributed equally, ranging from 0.24 for hypothetical TUDPD, to a high of 0.34 for temporal TUDPD. Response difficulty (RD) showed negative relation at -0.60 with coping feasibility (CF) and response efficacy (RE) showed positive relation with CF at 0.74. All of these paths were statistically significant at $p < 0.05$. Thus, according to Hair et al. (2010) we concluded good reliability scores for the higher order constructs, TuD and CF.

5.1.4 Paired and Independent Sample T-Tests

To test whether the concrete and the abstract scenarios presented to each of the two groups actually created difference in perception, a series of t-tests were performed, including both paired and independent sample t-tests. Table 16 summarizes the t-tests results. The paired t-test was performed to compare the difference between means of threat un-desirability, coping feasibility, and protection motivation within each group when respondents were presented concrete scenarios versus abstract scenarios. An independent sample t-test analysis was conducted to compare means of threat un-desirability, coping feasibility, and protection motivation for both groups during the first event and the second event. The first event included a concrete scenario presented to group one and an abstract scenario presented to group two. The second event included the presentation of an abstract scenario presented to group one and a concrete scenario presented to group two.

Table 16: T-Test Results Analysis

<table>
<tr><th colspan="4">Group 1 Paired T-Test</th></tr>
<tr><th>Construct</th><th>Concrete Mean (SD)</th><th>Abstract Mean (SD)</th><th>Mean Difference (Paired T-Statistic)</th></tr>
<tr><td>PM*</td><td>4.92 (0.63)</td><td>5.37 (1.08)</td><td>-.45 (-5.58)</td></tr>
<tr><td>TuD*</td><td>4.90 (0.96)</td><td>5.20 (1.03)</td><td>-.30 (-3.52)</td></tr>
<tr><td>CF</td><td>4.03 (0.76)</td><td>4.07 (0.78)</td><td>-.04 (-0.70)</td></tr>
<tr><th colspan="4">Group 2 Paired T-Test</th></tr>
<tr><th></th><th>Abstract Mean (SD)</th><th>Concrete Mean (SD)</th><th>Mean Difference (Paired T-Statistic)</th></tr>
<tr><td>PM*</td><td>5.50 (1.01)</td><td>5.65 (0.98)</td><td>-0.15 (-2.01)</td></tr>
</table>

TuD*	5.19 (0.86)	5.57 (1.01)	-0.38 (-4.70)
CF	4.33 (0.89)	4.30 (0.95)	+0.3 (0.50)
Mean Difference Across Groups (Independent T-Test Statistic)			
PM*	-.58 (-5.57)	-0.28(-2.18)	
TuD*	-.29(-2.54)	-0.37(-2.92)	
CF*	-.30(-2.98)	-0.22(-2.04)	

**P < 0.05*

On average, participants of group one showed change in their protection motivation when given a concrete threat context scenario (M = 4.92, SE = 0.06) compared to their protection motivation when given an abstract threat context scenario (M = 5.37, SE = 0.09). This difference, - 0.45, 95% CI [-0.60, -0.29], was significant t(130) = -5.58, p = 0.000, and represented an effect of d = -0.49. Similarly, participants showed change in their threat un-desirability perception (M = 4.90, SE = 0.08) compared to their perception when given an abstract threat scenario (M = 5.20, SE = 0.09). This difference, - 0.30, 95% CI [-0.47, -0.13], was also significant t(130) = -3.52, p = 0.001, and represented an effect of d = -0.3. However, change in coping feasibility perception was not significant. On average participants given a concrete scenario showed change in their coping feasibility perception (M = 4.03, SE = 0.07) compared to their perception when given an abstract scenario (M = 4.08, SE = 0.07). This difference, - 0.05, 95% CI [-0.18, -0.08], was not significant t(130) = -0.7, p = 0.49, and represented an effect of d = -0.07.

On average, group two participants showed changed in their protection motivation when given an abstract scenario for a specific threat context (M = 5.50, SE = 0.09) compared to their perception when given a concrete threat context scenario (M = 5.65, SE = 0.09). This difference, - 0.15, 95% CI [0.00, 0.29], was significant t(130) = 2.00, p =

0.047, and represented an effect of d = -0.17. Similarly, participants showed change in their threat un-desirability perception (M = 5.19, SE = 0.08) compared to their perception when given a concrete threat context scenario (M = 5.57, SE = 0.09). This difference, -0.38, 95% CI [0.22, 0.54], was significant t(130) = 4.70, p = 0.000, and represented an effect of d = -0.41. However, change in coping feasibility perception was not significant. On average, participants given an abstract scenario showed change in their coping feasibility perception (M = 4.34, SE = 0.08) compared to participants given a concrete scenario (M = 4.30, SE = 0.08). This difference, 0.04, 95% CI [-0.12, 0.2], was not significant t(130) = 0.5, p = 0.62, and represented an effect of d = 0.04.

On average, group one participants who were given concrete scenario showed change in protection motivation (M = 4.92, SE = 0.06) compared to group two participants who were given an abstract scenario (M = 5.50, SE = 0.09). This difference, -0.58, 95% CI [-0.79, -0.38], was significant t(260) = -5.57, p = 0.000, and represented an effect of d = -0.57. In addition, group one participants showed change in threat un-desirability perception (M = 4.90, SE = 0.08) compared to group two participants (M = 5.19, SE = 0.08). This difference, -0.29, 95% CI [-0.51, -0.06], was significant t(260) = -2.54, p = 0.012, and represented an effect of d = -0.34. Similarly, on average group one participants showed change in coping feasibility perception (M = 4.03, SE = 0.07) compared to group two participants (M = 4.33, SE = 0.08). This difference, -0.3, 95% CI [-0.51, -0.10], was also significant t(260) = -2.98, p = 0.003, and represented an effect of d = -0.34.

On average, group one participants who were given an abstract scenario showed change in protection motivation (M = 5.37, SE = 0.09) compared to group two participants who were given a concrete scenario (M = 5.65, SE = 0.09). This difference, -0.28, 95% CI [-0.53, -0.03], was significant t(260) = -2.18, p = 0.030, and represented an effect of d = -0.29. In addition, on average, group one participants showed change in threat un-desirability perception (M = 5.20, SE = 0.09) compared to group 2 participants (M = 5.57, SE = 0.09). This difference, -0.37, 95% CI [-0.61, -0.12], was significant t(260) = -2.92, p = 0.004, and represented an effect of d = -0.37. Similarly, on average group one participants showed change in coping feasibility perception (M = 4.08, SE = 0.07) compared to group two participants (M = 4.30, SE = 0.08). This difference, -0.22, 95% CI [-0.43, -0.01], was also significant t(260) = -2.04, p = 0.042, and represented an effect of d = -0.23. Table 6 shows a summary of both the independent t-test and the paired t-test results. The analysis of the results showed that hypothesis four and five are supported. Table 17 summarizes the two hypotheses subject of study one and the conclusion of data analysis results relevant to each presented hypothesis.

Table 17: Study One and Hypotheses Support

Hypothesis	Data Analysis Results
H4: The greater the threat un-desirability, the higher the protection motivation	Supported
H5: The greater the coping feasibility, the higher the protection motivation	Partially Supported

5.1.5 Model Comparative Analysis

This study included the performance of a comparative analysis. The purpose of this comparative analysis is to compare the traditional PMT model used in the context of information security to the model presented by this research. The performance of the traditional PMT model was measured by an instrument adopted from Johnston and

Warkentin (2010). The traditional use of PMT measured the impact of threat and coping appraisals on protection motivation. Threat vulnerability (Vul) and threat severity (Sev) constructs measured threat appraisal (TA). Three items, TVul1, TVul2, and TVul2 measured threat vulnerability. Four items, TSev1, TSev2, TSev3, and TSev4 measured threat severity. Response efficacy (RE) and self-efficacy (SE) constructs measured coping appraisal (CA). Three items, RE1, RE2, and RE3 measured response efficacy construct. Three items SEff1, SEff2, and SEff3 measured self-efficacy construct.

A confirmatory factor analysis (CFA) was performed to confirm the constructs measures. The results are only presented for reflective constructs. Software used is Smart-PLS version 3 (Ringle, 2015). The procedures used are partial least squares (PLS) and PLS bootstrapping (5000 runs). A bootstrap sample size of 5000 is recommended (Hair et al., 2011). The procedure of bootstrapping, which validates the model, involves drawing a large number of subsamples from the original sample to allow the significance of formative indicators' coefficients to be tested (Hair et al., 2010). The outer loadings were analyzed for all items measuring PMT constructs. All items showed high outer loading scores and P-values confirmed statistical significance of all items. Table 18 shows the outer loadings results for all items used.

Table 18: CFA Outer Loadings for Items of the PMT Original Model

Items	Outer Loadings	T Statistics (|O/STDEV|)	P Values
PM1 <- PM	0.80*	34.71	0.00
PM2 <- PM	0.86*	46.09	0.00
PM3 <- PM	0.87*	67.42	0.00
PM4 <- PM	0.46*	8.10	0.00
PM5 <- PM	0.86*	61.03	0.00

RE1 <- RE	0.90*	80.40	0.00
RE2 <- RE	0.93*	104.53	0.00
RE3 <- RE	0.89*	53.58	0.00
SEff1 <- SE	0.81*	35.11	0.00
SEff2 <- SE	0.90*	68.06	0.00
SEff3 <- SE	0.88*	62.19	0.00
TSev1 <- Sev	0.85*	62.55	0.00
TSev2 <- Sev	0.88*	102.97	0.00
TSev3 <- Sev	0.81*	34.87	0.00
TSev4 <- Sev	0.80*	30.06	0.00
TVul1 <- Vul	0.91*	77.49	0.00
TVul2 <- Vul	0.88*	66.12	0.00
TVul3 <- Vul	0.90*	70.43	0.00

**P < 0.05*

Following the factor analysis and the outer loadings of construct items, constructs reliability and validity was tested. The values for composite reliability, the Cronbach's Alpha, the average variance extracted (AVE), and discriminant validity were analyzed to evaluate constructs reliability and validity. Table 19 shows the values for Cronbach's Alpha, AVE, and composite reliability. The discriminant validity test was performed and the results was included in Table 19 as well.

Table 19: Constructs Reliability and Discriminant Validity for PMT Model

	Cronbach's Alpha	Composite Reliability	Average Variance Extracted AVE	PM	RE	SE	Sev	Vul
PM	0.83	0.89	0.62	**0.79**				
RE	0.89	0.93	0.81	0.41	**0.90**			
SE	0.83	0.90	0.75	0.32	0.55	**0.86**		

Sev	0.85	0.90	0.69	0.24	0.22	0.22	**0.83**	
Vul	0.88	0.92	0.80	0.11	0.08	0.11	0.56	**0.90**

Results analysis, as shown in the tables above support the reliability and validity of the constructs used in the traditional PMT approach. We also performed the HTMT test on the model. Table 20 summarizes the HTMT test results for the constructs. The results show that all values are below the HTMT critical value, which confirms constructs discriminant validity.

Table 20: HTMT Discriminant Validity Results for PMT Model

	PM	RE	SE	Sev
RE	0.47			
SE	0.38	0.64		
Sev	0.30	0.27	0.27	
Vul	0.14	0.09	0.13	0.63

Both models showed high scores while statistically significant. However, the variance explained by each model varied significantly. Table 21 shows comparison of the results for variance explained by each model.

Table 21: Variance Explained by Each Model

	Research Model		PMT Traditional Model	
	R Squared Adjusted	Q Squared	R Squared Adjusted	Q Squared
PM	0.34	0.20	0.19	0.11
	F Squared (CF)	F Squared (TuD)	F Squared (CA)	F Squared (TA)
	0.10	0.34	0.19	0.02

Also, Figures 7 and 8 show each model scores when measured by Smart-PLS.

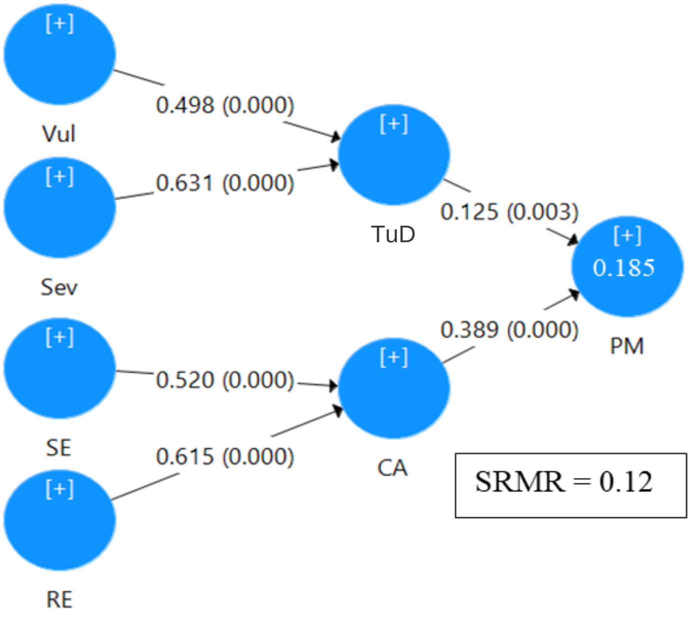

Figure 7. Smart-PLS traditional PMT model illustration

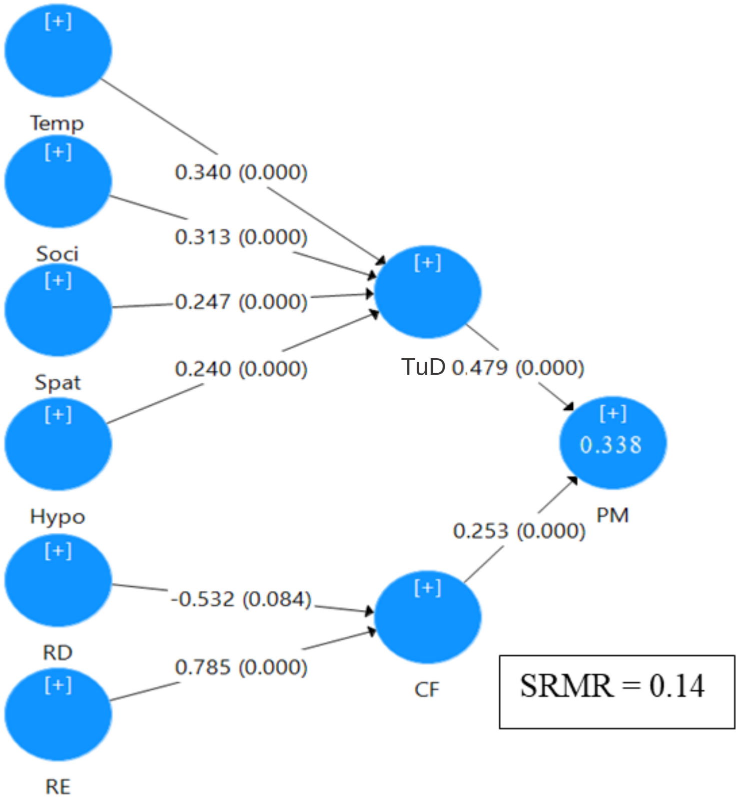

Figure 8. Smart-PLS study one model illustration

The original PMT model predicts that the change in coping appraisal and threat appraisal significantly influence protection motivation. The analysis of the results using the traditional PMT model shows that while both constructs, coping appraisal and threat appraisal, are statistically significant, coping appraisal has a moderate effect size of 0.19 and threat appraisal has a small effect size of 0.02. The analysis of the results also shows that coping and threat appraisals in the model explain 19 % of the variance in protection motivation. The model presented in this research predicts that change in coping feasibility and threat un-desirability significantly influence protection motivation. The analysis of the results for the model presented by this research shows that coping feasibility has a moderate effect size while threat un-desirability has a large effect size of 0.34. The analysis of the results also shows that coping feasibility and threat un-desirability explained 34% of the variance in protection motivation. The results show that the model presented in this research offers a larger effect size with a much greater explanatory power. This outcome supports the argument proposed in this research that this model is able to apply PMT based on its original intent that requires the perception of the threat to be on a personal level not against the organization. The data analysis of study one supports that the decreased desirability of the threat and the increased perception of the feasibility of the coping mechanism significantly influence protection motivation.

5.2 Study Two Data Analysis

The objective of study two is to test the entire research model. The model evaluates the impact of knowledge dimensions (breadth, depth, and finesse) on protection motivation, while fully mediated by the individual’s affective perception of threat un-desirability and coping feasibility. Study two will implement a cross-sectional web-based survey for data collection to test and measure the impact of all proposed research hypotheses.

5.2.1 Sample Frame and Used Sample

The sample frame for study two included currently employed full-time business professionals who use information systems for their daily jobs. The sample frame does not include labor workers who do not use enterprise information systems daily to accomplish their job-related tasks. The sample frame also does not include part-time, retired professionals, IT professionals, or professionals from technology companies. A professional company, Qualtrics, was contracted for the recruitment of participants and the administration of the online survey.

The company was contacted to provide 200 complete and usable responses. During the data collection process, a collaboration between the researcher and the company was followed to make sure all responses matched the sample frame criteria. The collaboration process included a soft launch to test the accuracy of the respondents screening process. Following the soft launch, the process of the full data collection was performed. During this process, the company provided a total of 247 responses. From the total provided responses, 28 responses were removed for being incomplete, inaccurate, or from respondents from technology companies. The total number of responses used for the data analysis was 219 responses from a diverse sample of currently employed full-time business professionals.

5.2.2 Descriptive Statistics

The used 219 usable responses included 75% females and 25% males. Almost all of the participants, 98%, were older than were 21 years of age. About 60% of the participants received a 4-year college degree or higher, 10% received an associate degree, 20% received some college education, and 10% received high school diploma. The majority of the participants, 52%, have been with their current company 6 years or more, 42% have been with their company between 1 to 5 years, and only 6% have been with their company for less than one year. Almost all of the participants, 97%, had some level of familiarity with computers, including 54% were extremely familiar with computers. Most of the participants, 81%, used computers all of the time to get their job tasks done. Descriptive statistics details are included in Appendix D.

5.2.3 Changes from Study One

The key measures used in study two were refined based on the data analysis performed in study one. Study one confirmed the use of most of the proposed key measures for threat un-desirability, coping feasibility, and protection motivation. However, the validity and reliability data analysis of the key measures supported the removal of two items. Specifically, study two did not include TUDPD_Hypo3 and TUDPD_Spat1. Also, study two included few refinements regarding terms used in the survey questions. The term “distant” was replaced with “far away” in study two survey. Additionally, the term “hypothetical” that was used in the instrument of study one was changed to “speculative” in instrument used for study two. Finally, because the sample frame of study two is different from the sample frame of study one, we included several additional statistical controls. We also changed the way threat context was communicated to the participants. Study one presented to participating students two concrete and abstract scenarios of specific threats. However, in study two, we asked the participating employees to select from a list of threats the threat that employees have heard about or have some experience with.

5.2.4 Statistical Controls

This study considered several control factors that could influence participants' protection motivation. Similar to study one, participants' gender, age, computer experience, and risk appetite were used as statistical controls. In addition, the study recognized that there are other statistical controls applicable to professionals that should also be analyzed. These controls are participants' industry type, department of work, level of education, years of work experience with current organization, and the level of technology use on the job. Consequently, we included these demographics characteristics as baseline statistical controls. Among all statistical controls, only computer experience and level of technology use were found to be statistically significant. To arrive at the optimal control variable model, the non-significant statistical controls were removed. The analysis of the control variables reveals that the level of computer experience and the level of technology use to perform work related duties impact protection motivation. Those two statistically significant controls accounted for 0.04 change in the independent variable. Table 22 shows the statistical significance and the impact of the control variables.

Table 22: Control Variables Statistics

Control Factors	Factor Loading	T Statistics	P Values

Age	-0.22	0.734	0.231
Computer Experience*	0.797	2.891	0.002
Department	0.146	0.443	0.329
Education	0.189	0.744	0.228
Experience	-0.073	0.248	0.402
Gender	0.076	0.286	0.387
Industry	-0.22	0.721	0.235
Technology Use*	0.707	2.309	0.01
Risk Appetite	0.03	0.47	0.32
PM Adjusted R-Square = 0.04			

**P > 0.05*

5.2.5 Construct Validity and Reliability

The validity and reliability of all constructs used in this study was tested. This study included constructs measuring the dimensions of knowledge, knowledge breadth (KB), knowledge depth (KD), and knowledge finesse (KF). It also included threat un-desirability (TuD), coping feasibility (CF), and protection motivation (PM). Knowledge dimensions constructs KB, KD, and KF were measured by three items respectively labeled (KB1, KB2, KB3), (KD1, KD2, KD3), and (KF1, KF2, KF3). The remaining constructs – threat un-desirability, coping feasibility, and protection motivation measures followed the items confirmed by study one. Table 23 shows the constructs loading scores.

Table 23: Items loadings with T-statistics and P-values (CFA)

	Items Loadings	T Statistics (|O/STDEV|)	P Values
Hypo1 <- Hypo*	0.85	29.33	0.00
Hypo2 <- Hypo*	0.86	36.68	0.00

Hypo3 <- Hypo*	0.28	2.01	0.02
KB_1 <- KB*	0.93	43.14	0.00
KB_2 <- KB*	0.96	97.18	0.00
KB_3 <- KB*	0.95	88.04	0.00
KD_1 <- KD*	0.95	88.95	0.00
KD_2 <- KD*	0.94	67.64	0.00
KD_3 <- KD*	0.93	62.54	0.00
KF_1 <- KF*	0.96	109.75	0.00
KF_2 <- KF*	0.96	148.38	0.00
KF_3 <- KF*	0.91	55.63	0.00
PM1 <- PM*	0.82	22.54	0.00
PM2 <- PM*	0.84	34.98	0.00
PM3 <- PM*	0.79	17.08	0.00
PM4 <- PM*	0.87	39.29	0.00
PM5 <- PM*	0.87	39.70	0.00
RD1 <- RD*	0.92	63.45	0.00
RD2 <- RD*	0.93	66.28	0.00
RD3 <- RD*	0.90	39.02	0.00
RE1 <- RE*	0.90	49.59	0.00
RE2 <- RE*	0.93	75.50	0.00
RE3 <- RE*	0.90	49.85	0.00
Soci1 <- Soci*	0.69	10.60	0.00
Soci2 <- Soci*	0.83	27.76	0.00
Soci3 <- Soci*	0.88	62.91	0.00
Spat1 <- Spat*	0.40	3.28	0.00
Spat2 <- Spat*	0.85	42.47	0.00
Spat3 <- Spat*	0.85	31.53	0.00
Temp1 <- Temp*	0.73	11.91	0.00
Temp2 <- Temp*	0.73	15.94	0.00
Temp3 <- Temp*	0.82	27.77	0.00

**P < 0.05*

As shown in table 23, all knowledge dimension items for KB, KD, and KF returned high loading scores. Also the loadings of all other remaining items for PM, the four dimensions of TuD (Temp, Soci, Spat, and Hypo), and the two dimensions of CF (RD and RE) all showed high loading scores consistent with study one. The table also show that all items were statistically significant with all P-Values less than 0.05.

Following the analysis of outer loadings, each construct reliability and validity was tested. The values for composite reliability, the Cronbach's Alpha, the average variance extracted (AVE), and discriminant validity were checked to evaluate constructs reliability and validity. Table 24 shows the values for Cronbach's Alpha, AVE, and composite reliability. The discriminant validity test was performed and results were included in Table 24 as well. The results of the discriminant validity, the diagonal values in boldface in the table, were greater than any of the internal factors correlations (or correlations of the constructs) for all constructs. All AVE and composite reliability values are indications of conversion validity. Also all Cronbach's Alpha values are high. Although the Cronbach's Alpha scores for the construct measuring psychological distance to threat un-desirability were slightly lower than 0.7, all other scores for these constructs such as loadings, composite reliability, AVE, and discriminant validity are high.

Table 24: Construct Reliability and Validity

	α	Composite Reliability	AVE	Hypo	KB	KD	KF	PM	RD	RE	Soci	Spat	Temp
Hypo	0.67	0.86	0.75	**0.87**									
KB	0.94	0.96	0.89	0.23	**0.94**								
KD	0.93	0.96	0.88	0.20	0.80	**0.94**							

KF	0.94	0.96	0.89	0.00	0.49	0.55	**0.94**						
PM	0.90	0.92	0.70	0.48	0.42	0.42	0.22	**0.84**					
RD	0.91	0.94	0.84	-0.01	0.06	0.10	0.36	-0.11	**0.92**				
RE	0.90	0.94	0.83	0.37	0.52	0.49	0.35	0.52	-0.06	**0.91**			
Soci	0.73	0.85	0.65	0.61	0.15	0.13	0.06	0.26	0.21	0.23	**0.81**		
Spat	0.62	0.84	0.72	0.66	0.26	0.21	0.06	0.41	0.09	0.32	0.74	**0.85**	
Temp	0.64	0.80	0.58	0.68	0.20	0.21	0.05	0.45	0.12	0.36	0.66	0.68	**0.76**

We also performed the HTMT discriminant validity test. The KB, KD, KF, RD, RE, and PM constructs values were below the HTMT critical values confirming discriminant validity. In addition, as expected with the psychological distance constructs, some of the values were slightly above the HTMT critical value. Because these are formative constructs and are expected to have cross loadings. These results were consistent with study one. Table 25 summarizes the HTMT test results.

Table 25: HTMT Discriminant Validity Test

	Hypo	KB	KD	KF	PM	RD	RE	Soci	Spat
KB	0.28								
KD	0.26	0.85							
KF	0.09	0.53	0.59						
PM	0.63	0.46	0.45	0.24					
RD	0.12	0.07	0.11	0.39	0.12				
RE	0.48	0.56	0.54	0.38	0.58	0.07			
Soci	0.87	0.17	0.15	0.08	0.32	0.26	0.29		
Spat	1.03	0.33	0.27	0.14	0.55	0.15	0.42	1.07	
Temp	1.03	0.24	0.27	0.11	0.59	0.21	0.46	0.95	1.05

5.2.6 Model Testing

Using the established controlled model, the effects of knowledge dimensions on the perception of threat un-desirability and coping feasibility were tested. Similarly, the effects of threat undesirability and coping feasibility on protection motivation were tested. Table 26 shows the statistical significance and the total effects of each construct in the model.

Table 26: Total Effects of Model Constructs

	Original Sample (O)	T Statistics (|O/STDEV|)	P Values
CF -> PM*	0.34	4.32	0.00
KB -> PM*	0.11	2.91	0.00
KB -> TuD*	0.27	3.55	0.00
KD -> CF*	0.41	5.43	0.00
KD -> PM*	0.14	3.17	0.00
KF -> CF*	0.18	1.70	0.04
KF -> PM*	0.06	1.61	0.05
TuD -> PM*	0.41	6.18	0.00

**P < 0.05*

As shown in the table, the results indicated that knowledge breadth was significant in influencing the perception of threat un-desirability. In addition, both knowledge depth and knowledge finesse were significant in their influence on the perception of coping feasibility. Consistent with study one, both threat un-desirability and coping feasibility significantly influenced protection motivation. Although the impact of coping feasibility on PM was significant, the path analysis of one of its formative constructs, RD, was not significant. Although RD is theoretically grounded and its factor analysis was significant with p-value less than 0.005, it did not provide significant impact towards CF. To further understand this outcome, we looked at studies addressing task complexity as it relates to RD. Gill and Hicks (2006) explained that task complexity contains four other views in addition to the psychological state or individual perception. The other views of task complexity are information processing, structure, problem space, and task characteristics. Therefore, future research should be continue to explore the impact of the other four views on CF.

Table 27 shows the variance explained by the research model. The analysis of the results using the research model show that knowledge breadth has a small effect size on threat un-desirability. Similarly knowledge fenisse has a small effect size on coping feasibility while knowledge depth has a moderate effect size on coping feasibility. Results show that both constructs, threat un-desirability and coping feasibility, each has a moderate effect size of 0.23 and 0.16 respectively. The analysis of the results also shows that threat un-desirability and coping feasibility in the model account for 39 % of the variance in protection motivation.

Table 27: Variance Explained by the Research Model

PM		TuD		CF	
R Square Adjusted	Q Squared	R Square Adjusted	Q Squared	R Square Adjusted	Q Squared
0.39	0.25	0.07	0.04	0.27	0.13
F Square (TuD)	F Square (CF)	F Square (KB)		F Square (KD)	F Square (KF)
0.23	0.16	0.08		0.16	0.03

The test of the research model indicated that the model fit (SRMR) value is 0.088. The fit scores, as well as the adjusted R square and the p-values, show that the model is significantly improved and capable of predicting a statistically significant influence of threat un-desirability and coping feasibility on protection motivation. These findings suggest that knowledge dimensions can form the personal perception of threat un-desirability and coping feasibility, which in turn are sufficient and significant to influence the motivation to protect information. Figure 9 shows the path coefficients and the statistical significance of model’s constructs.

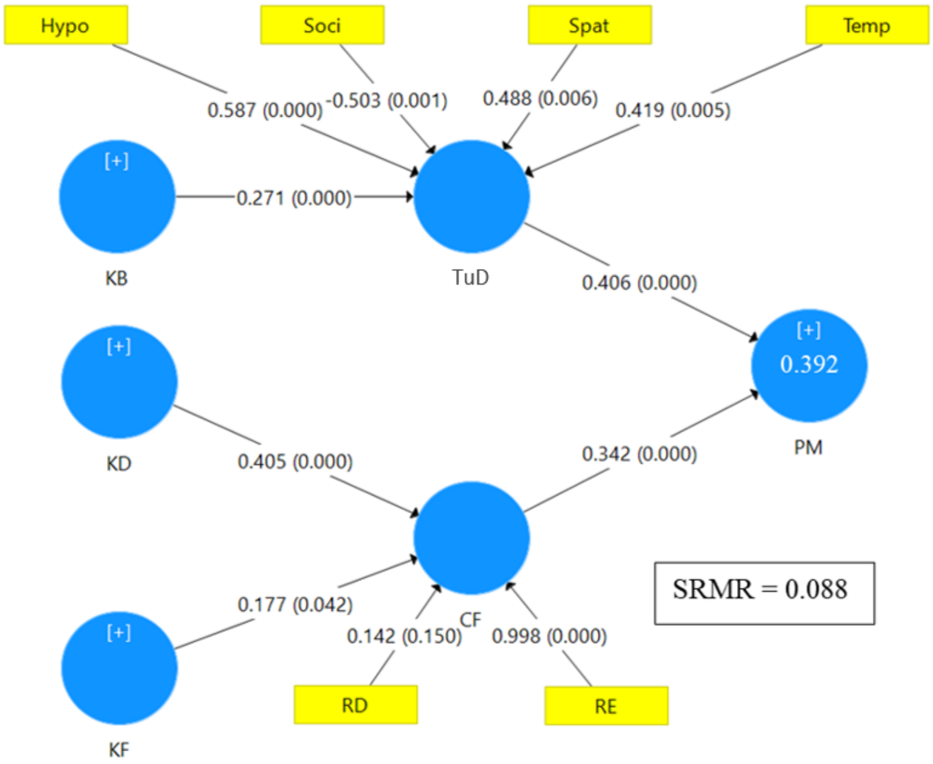

Figure 9. Model path coefficients and significance

The analysis of the results show that all proposed hypotheses are supported. Table 28 summarizes all hypotheses presented by this research and the conclusion of data analysis results relevant to each presented hypothesis.

Table 28: Research Hypotheses and Results Support for Study Two

Hypothesis	Data Analysis Results
H1: The greater the breadth of knowledge in knowledge mechanisms, the greater the un-desirability of the threat by end-users	Supported
H2: The greater the depth of knowledge in knowledge mechanisms, the higher the coping feasibility	Supported

H3: The greater the finesse, the higher the coping feasibility	Supported
H4: The greater the threat undesirability, the higher the protection motivation	Supported
H5: The greater the coping feasibility, the higher the protection motivation	Supported

CHAPTER 6 – DISCUSSION

This chapter discusses interpretation of the results, limitations, contributions, and future research directions. The chapter starts with the discussion of the data results and its support to the research objectives and the proposed hypotheses. Following the results discussion, we address research limitations and the way these limitations were addressed. We then explain the research contributions to scholarly academic researchers and to practitioners based on data findings and the supported hypotheses. We will explain how these findings contribute to further the work of academicians and practitioners. We follow by discussing future directions of information systems research in the context of information security. Finally, we finish with our conclusion from this research.

6.1 Interpretation of Results

This research sought to understand the way knowledge mechanisms, such as SETA and security policies, influence employees' secure behavior in a particular threat context. Threat context represented the events or conditions that expose information systems to potential threats. The research conceptualized knowledge mechanism across three dimensions: breadth, depth, and finesse. The research also conceptualized the psychological process, to preserve the intent of PMT, based on the threat un-desirability and coping feasibility. The four dimensions of the psychological distance, temporal, social, spatial, and hypothetical dimensions, formed the threat un-desirability higher order construct (HOC). Similarly, response difficulty and response efficacy formed the coping feasibility HOC.

6.1.1 Study One Findings

Study one measured how individuals' psychological distance from a specific threat forms the perception of threat un-desirability and coping feasibility. The psychological distance from the threat was manipulated in terms of the concreteness or abstractness of a specific threat context. The study also measured the impact of threat un-desirability and coping feasibility on protection motivation. Results show that the concreteness or abstractness of a threat context actually creates a significant difference in individuals' perception regarding threat un-desirability and coping feasibility. Results also show that threat un-desirability and coping feasibility significantly influence protection motivation.

We found that the abstractness or concreteness of a threat context cause change in the perception of threat un-desirability. That change was significant across all four psychological dimensions. As we argued, grounded by CLT, that variation along any dimension of psychological distance influenced the perception of threat un-desirability. The concrete threat context, manipulated across all four dimensions, increased the perception of threat un-desirability. The change was consistent when compared the results within a group or between the two groups. This supports the idea that the un-desirability of the threat will increase when individuals perceive the threat on a closer psychological distance. This is consistent with the original intent of PMT. Therefore, as we proposed, the affective perception of threat un-desirability will preserve the original intent of PMT in the context of information security.

An interesting finding related to the hypothetical dimension of the psychological distance is worth mentioning. The results of the hypothetical dimension were statistically significant with high scores for reliability and validity. However, we found that this psychological dimension provided slightly lower contribution to the change in the HOC, threat un-desirability, compared to the other three dimensions of the psychological distance. We interpreted this to be due to the difficulty of manipulating a true and popular information security threat as hypothetical threat that is less likely to happen. The application of this finding will be addressed in more details in the implication section.

Findings regarding coping feasibility showed different results within groups as compared to between groups. The change in coping feasibility was not significant within each group when the threat context was presented in two sequential events alternating abstractness and concreteness of threat context. We interpreted this to be a result of the learning experience. Once a group receives knowledge about a threat and its mitigating action, whether in concrete or abstract fashion, any subsequent communication will provide additional knowledge, and the perception of the coping feasibility change will not be statistically significant. In contrast, there was a significant change in the perception of coping feasibility between groups. When we simultaneously presented an abstract threat context to one group and a concrete threat context to another group and compared the results, we found significant change in perception regarding coping feasibility between the two groups. The group that received concrete threat context showed higher scores for the coping feasibility HOC compared to the group that received an abstract context. This outcome supported our argument that the perception of the coping feasibility will increase when an individual receives concrete knowledge about the context of that threat.

Participants in both groups showed positive change in their protection motivation when they received knowledge about information security threat. Results showed that the positive change in protection motivation was significantly higher for the participants of the group that received a concrete scenario compared to the group that received an abstract threat. The results showed that coping feasibility and threat un-desirability positively influence protection motivation. We found that as the perception of the threat un-desirability increases, the more motivated the individual would be to follow secure behavior. Similarly, we found that as the perception of the coping feasibility increases, the more motivated the individual would be to follow secure behavior. However, the results supported that threat un-desirability has the larger impact on protection motivation. Thus, this is consistent with our argument that despite the importance of cognition, behavioral drivers are affective.

In conclusion, the findings from study one supported that concreteness or abstractness of threat context will actually influence the perception of threat un-desirability and coping feasibility. The concreteness of the threat context will increase the perception of threat un-desirability and coping feasibility. In addition, results support the positive impact of threat un-desirability and coping feasibility on protection motivation.

6.1.2 Study Two Findings

Study two measured the impact of knowledge dimensions (breadth, depth, and finesse) on protection motivation, while fully mediated by the employees' affective perception of threat un-desirability and coping feasibility. The results show support to the proposed positive impact of knowledge dimensions on the perception of threat un-desirability and coping feasibility. Similarly, results support the positive impact of threat undesirability and coping feasibility on protection motivation.

We found that knowledge breadth was significant in influencing the perception of threat un-desirability. The variety of knowledge provide broader understanding of the threat context. Breadth of knowledge will explain information security threats from external hackers, competitors, and natural disasters, as well as the internal threats caused by employees' behavior, whether malicious or accidental. The breadth of knowledge increase employees' abilities to recognize from a personal perspective the range of threats and associate security risks that employees my face during their daily responsibilities. The personal understanding of the damaging details of the threat will increase threat un-desirability. Therefore, as proposed, breadth of knowledge provided a significant positive influence on the employees' perception of threat un-desirability.

We also found that both knowledge depth and knowledge finesse were significant in their influence on the perception of coping feasibility. Understanding the details in depth about the available course of action will increase coping feasibility. The contribution of both completeness of knowledge about a threat and the ability to apply innovativeness and creativity positively affect the perception of the feasibility of the coping mechanism. The understanding of the complete steps needed to address any threat in a specific context while allowing employees to contribute with experience and creativity will reduce the perception of response difficulty and increased the perception of response efficacy. Therefore, both knowledge depth and finesse was found to positively influence coping feasibility.

Consistent with study one, we found that both threat un-desirability and coping feasibility significantly influenced protection motivation. Results show that threat un-desirability and coping feasibility provided significant positive influence on protection motivation. Therefore, we conclude that all proposed hypotheses of knowledge dimensions are supported. Knowledge breadth, depth and finesse are key factors in forming the personal perception of threat un-desirability and coping feasibility, which in turn are sufficient and significant to influence the motivation to protect information.

6.2 Limitations

We acknowledge the limitations that faced this research. Study one faced limitations due to the use of the experimental design and the sample representativeness. In addition, study one faced limitation due to the failure to manipulate response difficulty among participants. Study one was an experiment with university students conducted to understand perceptions toward information security threats. The use of an experiment with students presents concerns about the external validity of the study and the use of students to represent employees' responses. Similarly, some limitations also apply to study two. Study two followed a cross-sectional web-based survey for data collection. The limitations of study two were associated with the use of a survey instrument, which presents concerns regarding internal validity and reliability of results. The following section explains how we addressed these limitations.

Conducting an experiment with students could present a limitation to the generalizability of the study and extending its conclusions to employees. However, research supported the use of students in the context of information security as a reliable sampling frame. Students are members of an organization with valuable information assets and are subject to protection motivation factors similar to any system user (Warkentin et al., 2016). We accepted these limitations, as the literature supports the use of students as a reliable sample frame. Additionally, we were able to overcome the limitation of sample representativeness by presenting students with realistic information security threats relevant to university students. This allowed students to become information systems end users who have valuable information that should be protected. Therefore, the results were realistic and represented accurate useful measures of perceptions, and not just a proxy to professionals.

Another external validity concern may come from how realistic the manipulations of the experiment were in creating situations comparable to situations that employees may encounter in their organizations. To increase the realistic perception of the experiment manipulations, study one was designed to present several situations that students may encounter in their daily routines similar to what the employees may encounter in work environment. Study one required the communication of abstract and concrete realistic threat scenarios to construe threat perception on a higher or lower psychological distance from the end user. Using multiple threat scenarios allowed the study to overcome this concern. Covering multiple threat contexts between two groups of students allowed the study to measure the impact of a realistic threat context on participants' affective perception of that threat's un-desirability and coping feasibility. Only the manipulation of response difficulty was not successful. We found that response difficulty is a complex construct with different facets that can contribute to the perception of response difficulty. We acknowledge this limitation and encourage future research to explore facets of task complexity.

In conclusion, the experiment with students conducted in study one presented some limitations. However, these limitations are not different from any other research method. Also, many research studies used experiments when a convenience sample is possible with naturally formed groups such as students in a classroom (Creswell, 2014). Experiment, like the other methods, has several advantages. One of the most important of these advantages is the strength of internal validity of results. Therefore, experiments provide a powerful measurement with strong internal validity when used appropriately (S. Gupta, 2006; Poole & DeSanctis, 2004).

Limitations that faced study two were associated with the use of a survey instrument. The limitations here are similar to any study utilizing surveys for data collection and analysis. Surveys present concerns regarding internal validity and reliability of results. This stems from concerns regarding key measures, as well as a lack of consistency or accuracy in the provided responses. To mitigate the concerns regarding key measures, study two utilized validated measures used in prior literature. Also, study two followed scientific statistical processes to confirm constructs validity and reliability. The study also included several statistical controls to eliminate factors that might offer competing external explanations.

Study two followed the recommended survey structure and length as explained by Hair et al. (2010), to enable accurate and consistent responses. Also, the study followed strict criteria to eliminate incomplete or inaccurate responses. Finally, to complete the data collection from a wide range of professionals, we contracted a professional company to distribute the survey and collect the responses. Although this decision may cause a concern regarding the researchers' control over the sample and the collected responses, this approach is supported in the literature. Further, the benefits of using professional survey provider was extensively discussed and explained (Creswell, 2014; Sue & Ritter, 2007). Additionally, we provided to the contracted company a specific sample frame and response collection criteria. The contracted data collection company provided the researchers full access to the process to verify the sample frame and responses quality. We rejected any responses that did not perfectly match the sample frame or did not meet the response quality criteria. Literature supports the use of surveys, as they offer economical access to large cross-sectional participants from the desired sample frame, which increases the statistical power (Creswell, 2014).

All limitations were accepted and addressed appropriately. In addition, these limitations can be viewed as opportunities for future research. Some of these opportunities for future research will be discussed in a subsequent section.

6.3 Contribution

This research presented a theoretically grounded model that addresses current gaps in the information security literature. The information security literature did not explicitly leverage knowledge dimensions. We developed a unique study in the context of information security to measure the impact of knowledge dimensions on affective perception of security threats. The research offers greater understanding of how knowledge dimensions influence employees' psychological state to motivate compliance. The model presented in this research explains various application of knowledge dimensions in SETA programs and information security policies. Understanding the unique outcomes to each of the knowledge dimensions provide strategies regarding the use of knowledge mechanisms in the context of information security.

Business experts advise that organizations should stay current and expand their abilities to provide information security insights regarding broader security threats, as well as security threats that are specific to the organization and its environment (Accenture, 2018). This research presents a supported scientific approach to enable organizations to provide either broader or more specific information security insights. This research explains the strategic applications of knowledge dimensions, breadth, depth, and finesse. Breadth of knowledge can address the broader security threats that any employee or organization could face. At the same time, the model also explains how depth and finesse of knowledge can provide the needed accurate insights regarding specific organizational security threats.

The breadth of knowledge brings the personal perspective to information security threats. It enables organizations to provide insights regarding security threats, not only to protect the organization, but also to protect the employees themselves. Employees will understand the common threats that any business environment with digital assets may face. Our results support that breadth of knowledge will provide the needed perspective to keep employees vigilant regarding wide range security threats otherwise would be perceived irrelevant. It illustrates threats on a personal level as it becomes relevant to each employee and their line of business. Breadth of knowledge will allow employees to understand the degree of harm associated with security threats, which influence employees to see security threats as personal threats not as someone else’s problem. The broader understanding of information security threats will enable employees to connect the new and evolving threats with the existing and known information security threats. Breadth of knowledge will prevent the false sense of invulnerability and will motivate employees to follow secure behavior as their personal behavioral choice.

Our results also supports that depth and finesse of knowledge will increase the perception of response feasibility. Depth of knowledge provides understanding to actual and specific threats. That will reduce mistakes and will enable fast and accurate secure behavior to prevent or mitigate specific threatening situations. Depth of knowledge will increase the feasibility of security requirements. Because such deep understanding will reduce the conflict between security demands and job requirements. Depth of knowledge will support employees to perform their daily assignments while following secure behavior. Finesse allows the applications of comprehension and understanding of security threats gained from historical events and prior experiences to mitigate security incidents. Information security threats are increasing and advancing. Utilizing knowledge dimensions enables organizations to take a more effective approach to mitigate the increasingly diverse and sophisticated information security threats.

This research also provides a practical business approach to a traditionally technical topic. The application of knowledge across these three dimensions will help provide guidelines that are more specific to practitioners. Each industry faces different threats, and successful security countermeasures come from understanding these industry specific threats (Verizon, 2018). Therefore, the generic “one-size-fits-all” approaches are ineffective, especially with ambiguous or unknown security threats. This research shows the way to clarify threat contexts and the circumstances that may influence employees’ psychological state. Our model can inform organizational leaders and allow them to create policies and SETA programs tailored to employees' specific domains and level of knowledge. Knowledge dimensions will provide strategic understanding to inform the construction of security policies and SETA programs. Organizational leaders can design security policies and SETA programs with feasibility and on a personal level. The model explains the use of knowledge dimensions to focus employees' perceptions on response feasibility and threat un-desirability. The model allows the creation of feasible and desirable security strategies that are generalizable across different known threats as well as new threats that may emerge.

This research provides greater understanding regarding the impact of the various dimensions of knowledge. Understanding the influence of the breadth, depth, and finesse of knowledge on employees' perception allows managers to create security policies and SETA programs that align business goals and security requirements. Breadth of knowledge can reduce accidental security threats. It provides broader understanding that allows employees to understand security threats relevant to their daily and personal activities. Knowledge depth increases the accuracy of response implementation and motivates secure behavior. Finesse is a dimension of knowledge that has not been considered in the context of information security. Organizations often limit employees' ability to implement finesse in their response to mitigate a threat. This research provides support to the proposed positive impact of finesse dimension of knowledge. We provide a unique contribution to allow organizations to recognize the potential of this untapped dimension of knowledge. The mining of employees' insights can improve the way organizations evaluate feasibility of responses to security threats. Allowing employees to collaborate and brainstorm will positively influence the perception of the feasibility of secure behaviors.

This research offers noteworthy contributions to the literature. The research contributes by providing a more improved model of information security. The research model shows how to influence protection motivation in a way that limits results variations and allows PMT to work as designed in the context of information security. We also provide a theoretically driven re-conceptualization of PMT's constructs to preserve its intent. The conceptualization of PMT's constructs was accomplished by the application of CLT to explain employees' psychological process. CLT explained the way individuals will construe information security threats on a personal level. We were able to influence greater change in protection motivation by directing employees' perception to threat un-desirability and coping feasibility. Such a re-conceptualization of PMT's constructs allows the presentation of information security threats on a personal level.

The original context of PMT refers to a threat appraisal as the individuals' assessment of their own safety if they follow a certain behavior (Maddux & Rogers, 1983). However, the applications of PMT in the context of information security measured threat appraisal by how well an individual understands organizational threat, not personal safety. The position of the threat was removed from a personal threat and became an organizational threat. Threat un-desirability differs from threat appraisal in the context of information security. Threat un-desirability refers to the extent to which an individual will perceive a personal impact by the threat. The perception of the threat is based on the individual's psychological distance from the threat. Therefore, threat un-desirability re-conceptualizes PMT's threat appraisal in the context of information security to preserve the original intent of the theory and places the locus on the individual.

Similarly, the re-conceptualization of coping feasibility refers to the process by which individuals evaluate the effectiveness of the available risk mitigating behavior. Feasibility consideration focuses on the level of difficulty regarding the mitigating action. The model presented in this research shows that the increased knowledge depth and finesse will direct employees' perceptions towards the feasibility of the response mechanism. The locus of coping appraisal is the task to be performed by the individual. The locus of coping feasibility is the individual. Coping feasibility is concerned with the individual's perception of the ease (difficulty) in performing an action. Therefore, threat desirability re-conceptualizes the PMT's coping appraisal in the context of information security by focusing individuals' perception on the response appraisal from the feasibility perspective (response feasibility).

The research presents a theoretically grounded model that allows PMT to explain the psychological process of protection motivation. This model extends the theory while preserving its original intent that requires the perception of the threat to be on a personal level and not against the organization. The model offers a larger effect size with a much greater explanatory power.

This research provides a generalizable business approach for any incident-driven behavior that was typically viewed as a technical topic. The presented model allows the research to be generalizable across different known threats, as well as new threats that may emerge. The approach presented in this research focused on understanding the psychological process of any threat context, whether the threat is external, internal, malicious, or accidental. The context of the threat could be known and addressed by the organization, known but not addressed yet in organizational policies, or unknown and ambiguous. Context of information security threats clarify threatening circumstances and influence perception. The context of information security threats enable employees to distinguish between threats and follow secure behavior.

6.4 Future Research Directions

This research explored the impact of coping feasibility on protection motivation. The HOC was formed by response efficacy and response difficulty. We found that response difficulty is a multi-faceted construct. The literature shows that information processing, structure, problem space, and task characteristics are different facets that can contribute to the perception of task complexity (Gill & Hicks, 2006). Therefore, future research should continue to explore the impact of the other dimensions of task complexity on coping feasibility.

This study provides a reconceptualization to the psychological process of PMT. One of our objectives was to increase the generalizability of the model. The study focused on the affective attributes as the main drivers of behavior. The different components of PMT were conceptualized at different levels, i.e. task / context and individual. Such re-conceptualization extends the opportunity for researchers to use the re-conceptualized constructs of PMT in different domains beyond information security. This generalizable approach presents opportunities for future research to study persuasive communications for any incident-driven behavior, including PMT’s original domain.

Furthermore, we presented the influence of knowledge dimensions on protection motivation. Previous research discussed the importance of the comprehensiveness of knowledge in information security policies and SETA programs without explaining whether that means depth, breadth, or finesse of knowledge. This research presented support to the specific impact of the three knowledge dimensions of breadth, depth, and finesse on the perception in terms of un-desirability and feasibility. Researchers may pursue the application of this research model in a more specific approach. Therefore, future research may study content design and structure of policy or SETA programs in light of these specific knowledge dimensions.

6.5 Conclusion

This research presented a theoretically grounded model to understand how knowledge mechanisms such as policies and SETA programs influence employees' secure behavior in a particular threat context. The research model addressed several gaps in information security literature. Information security literature did not explicitly leverage knowledge dimensions. The model presented in this research explains various application of knowledge dimensions breadth, depth, and finesse in SETA programs and information security policies. In addition, the conventional application of PMT in the field of information security caused inconsistent and conflicting results. The research presents an improved model that preserves the original intent of PMT in the context information security to limit the variation of results. Finally, the research presented a generalizable approach for any incident-driven behavior and a practical business approach to a traditionally technical topic.

To support the proposed hypotheses and to test the research model, this research applied quantitative methods and examined the relationships between variables to address the research questions. The research empirically tested the model using two-study approach. The first study was a scenario-based experiment with 262 students. The experiment understood key psychological processes of threat perception. The second study empirically validated the entire theoretical model. We surveyed 219 employees across the organization with varied responsibilities and technical competence. We tested the theoretical model using structural equation modeling (SEM) approach.

Results show support to our proposal that the psychological distance from the threat allows employees to perceive the personal impact of the threat. When threat context was constructed on a closer psychological distance, the perception of threat un-desirability and coping feasibility increased. Results support that the key psychological constructs, threat un-desirability and coping feasibility, influence employees behavioral choices. Threat un-desirability focuses employees’ perception on un-desirable harmful outcomes of information security threats, while coping feasibility considerations direct employees’ perceptions towards action alternatives to protect the information. Threat un-desirability and coping feasibility showed significant positive impact on protection motivation.

Finally, this research study provided several contributions and set directions for future research. This research provided an improved model that explained protection motivation. The research proposed an approach to limit PMT results’ variations in the context of information security. Additionally, the study offered practitioners a business approach to a traditionally technical topic and researchers a generalized model to address known threats as well as new threats that may emerge.

REFERENCES

Ab Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *computers & security, 49*, 45-69.

Accenture. (2018). Cyber Threat-scape Report 2018: Midyear Cybersecurity Risk Review Retrieved from https://www.accenture.com/t20180803T064557Z__w__/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf#zoom=50

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS quarterly*, 107-136.

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems, 25*(4), 364-390.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312.

Ashenden, D. (2008). Information security management: A human challenge? *Information security technical report, 13*(4), 195-201.

Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). *Recent Trends in Network Security and Applications*, 420-429.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review, 84*(2), 191-215.

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

Bierly, P., & Chakrabarti, A. (1996). Generic knowledge strategies in the US pharmaceutical industry. *Strategic management journal, 17*(S2), 123-135.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do Systems Users have to Fear? using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS quarterly, 39*(4), 837-864.

Branscombe, N. R., Ellemers, N., Spears, R., & Doosje, B. (1999). The context and content of social identity threat. *Social identity: Context, commitment, content*, 35-58.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548.

Burns, A., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68*, 190-209.

Campbell, D. T., & Stanley, J. C. (1963). Experimental and quasi-experimental designs for research. *Handbook of research on teaching. Chicago, IL: Rand McNally*.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. *Journal of Management Information Systems, 31*(4), 49-87. doi:10.1080/07421222.2014.1001257

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11-19.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188. doi:10.2753/MIS0742-1222290305

Cohen, J. (1988). Statistical power analysis for the behavioral sciences. 2nd. In: Hillsdale, NJ: erlbaum.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.): Sage publications.

Crossler, R. E. (2010, 2010). *Protection motivation theory: Understanding determinants to backing up personal data.* Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on.

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

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of*

Management Information Systems, 31(2), 285-318. doi:10.2753/MIS0742-1222310210

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

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *computers & security, 49*, 162-176. doi:http://dx.doi.org.proxy.kennesaw.edu/10.1016/j.cose.2014.12.006

De Luca, L. M., & Atuahene-Gima, K. (2013). *Market knowledge dimensions and cross-functional collaboration: Examining the different routes to product innovation performance*.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449-457.

Ernst, & Young. (2016). *EY's 19th Global Information Security Survey 2016-17*. Retrieved from

Fenz, S., & Ekelhart, A. (2009). *Formalizing information security knowledge.* Paper presented at the Proceedings of the 4th international Symposium on information, Computer, and Communications Security.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology, 30*(2), 407-429.

Fowler Jr, F. J. (2013). *Survey research methods*: Sage publications.

Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management, 7*(1, 2), 159-180.

Fujita, K., Eyal, T., Chaiken, S., Trope, Y., & Liberman, N. (2008). Influencing attitudes toward near and distant objects. *Journal of Experimental Social Psychology, 44*(3), 562-572.

Gallivan, M. J. (2003). The influence of software developers' creative style on their attitudes to and assimilation of a software process innovation. *Information & Management, 40*(5), 443-465.

Galunic, D. C., & Rodan, S. (1998). Resource recombinations in the firm: Knowledge structures and the potential for Schumpeterian innovation. *Strategic management journal*, 1193-1201.

Garris, R., Ahlers, R., & Driskell, J. E. (2002). Games, motivation, and learning: A research and practice model. *Simulation & gaming, 33*(4), 441-467.

Gill, T. G., & Hicks, R. C. (2006). Task complexity and informing science: A synthesis. *Informing Science, 9*, 1.

Griffith, T. L., & Dougherty, D. J. (2001). Beyond socio-technical systems: introduction to the special issue. *Journal of Engineering and Technology Management, 18*(3), 207-218.

Gupta, B., Iyer, L. S., & Aronson, J. E. (2000). Knowledge management: practices and challenges. *Industrial management & data systems, 100*(1), 17-21.

Gupta, S. (2006). *Longitudinal investigation of collaborative e-learning in an end-user training context.* uga,

Gupta, S., Bostrom, R. P., & Huber, M. (2010). End-user training methods: what we know, need to know. *ACM SIGMIS Database, 41*(4), 9-39.

Hair, J. F., Black, W., Babin, B., & Anderson, R. (2010). Multivariate Data Analysis Seventh Edition Prentice Hall.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (1998). *Multivariate data analysis* (Vol. 5): Prentice hall Upper Saddle River, NJ.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice, 19*(2), 139-152.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the academy of marketing science, 40*(3), 414-433.

Halamish, V., Borovoi, L., & Liberman, N. (2017). The antecedents and consequences of a beyond-choice view of decision situations: A construal level theory perspective. *Acta psychologica, 173*, 41-45.

Hendrickson, A. R., Massey, P. D., & Cronan, T. P. (1993). On the test-retest reliability of perceived usefulness and perceived ease of use scales. *MIS quarterly*, 227-230.

Herath, T., & Rao, H. R. (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. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6

Ho, C. K. Y., Ke, W., & Liu, H. (2015). Choice decision of e-learning system: Implications from construal level theory. *Information & Management, 52*(2), 160-169.

Huang, N., Burtch, G., Hong, Y., & Polman, E. (2016). Effects of multiple psychological distances on construal and consumer evaluation: A field study of online reviews. *Journal of consumer psychology, 26*(4), 474-482.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *computers & security, 31*(1), 83-95. doi:http://dx.doi.org/10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly, 34*(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric. *MIS quarterly, 39*(1), 113-134.

Kanten, A. B. (2011). The effect of construal level on predictions of task duration. *Journal of Experimental Social Psychology, 47*(6), 1037-1047.

Kappelman, L., Nguyen, Q., McLean, E., Maurer, C., Johnson, V., Snyder, M., & Torres, R. (2017). The 2016 SIM IT Issues and Trends Study. *MIS Quarterly Executive, 16*(1), 47-80.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems, 12*(8), 518.

Kessel, P. v., & Allan, K. (2015). *EY's Global Information Security Survey*. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *computers & security, 28*(7), 493-508.

Köhler, C. F., Breugelmans, E., & Dellaert, B. G. C. (2011). Consumer acceptance of recommendations by interactive decision aids: The joint role of temporal distance and concrete versus abstract communications. *Journal of Management Information Systems, 27*(4), 231-260.

Krishna, A. (2012). An integrative review of sensory marketing: Engaging the senses to affect perception, judgment and behavior. *Journal of consumer psychology, 22*(3), 332-351.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS quarterly*, 71-90.

Liberman, N., & Trope, Y. (1998). The role of feasibility and desirability considerations in near and distant future decisions: A test of temporal construal theory. *Journal of personality and social psychology, 75*(1), 5.

Liberman, N., Trope, Y., & Wakslak, C. (2007). Construal level theory and consumer behavior. *Journal of consumer psychology, 17*(2), 113-117.

Liviatan, I., Trope, Y., & Liberman, N. (2008). Interpersonal similarity as a social distance dimension: Implications for perception of others' actions. *Journal of Experimental Social Psychology, 44*(5), 1256-1269.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS quarterly, 16*(2), 173-186.

Luca, L. M. D., & Atuahene-Gima, K. (2007). Market knowledge dimensions and cross-functional collaboration: Examining the different routes to product innovation performance. *Journal of marketing, 71*(1), 95-112.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Mathews, L. (2016). *Homeland Security Chief Cites Phishing As Top Hacking Threat*. Retrieved from Online: https://www.forbes.com/sites/leemathews/2016/11/29/homeland-security-says-phishing-biggest-hacking-threat/#46d404c01978

Mills, A., & Chin, W. (2007). Conceptualizing creative use: an examination of the construct and its determinants. *AMCIS 2007 proceedings*, 289.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward A Unified Model Of Information Security Policy Compliance. *MIS quarterly, 42*(1), 285.

Munro, M. C., Huff, S. L., Marcolin, B. L., & Compeau, D. R. (1997). Understanding and measuring user competence. *Information & Management, 33*(1), 45-57.

Nambisan, S., Agarwal, R., & Tanniru, M. (1999). Organizational mechanisms for enhancing user innovation in information technology. *MIS quarterly*, 365-395.

Nonaka, I., Byosiere, P., Borucki, C. C., & Konno, N. (1994). Organizational knowledge creation theory: a first comprehensive test. *International Business Review, 3*(4), 337-351.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *computers & security, 31*(5), 673-680.

Ponemon Institute. (2017). 2017 Cost of Data Breach Study: Global Overview. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

Poole, M. S., & DeSanctis, G. (2004). Structuration theory in information systems research: Methods and controversies. *The handbook of information systems research*, 206-249.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders’ Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems, 32*(4), 179-214. doi:10.1080/07421222.2015.1138374

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS quarterly, 37*(4), 1189-A1189.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757-778.

Ringle, C. M., Wende, Sven, & Becker, Jan-Michael. (2015). SmartPLS 3. In. Bönningstedt: SmartPLS. Retrieved from http://www.smartpls.com.

Rogers, R. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security, 56*, 70-82.

Sanchez, R. (1997). Managing articulated knowledge in competence-based competition. In R. Sanchez & A. Heene (Eds.), *Strategic Learning and Knowledge Management* (pp. 163-187). New York: Wiley.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341.

Siponen, M., Baskerville, R., & Heikka, J. (2006). A design theory for secure information systems design methods. *Journal of the Association for Information Systems, 7*(1), 31.

Siponen, M., & Iivari, J. (2006). Six Design Theories for IS Security Policies and Guidelines. *Journal of the Association for Information Systems, 7*(7), 445-472.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly, 34*(3), 487.

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems, 23*(3), 289-305.

Sitkin, S. B., & Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management Journal, 38*(6), 1573-1592.

Soderberg, C. K., Callahan, S. P., Kochersberger, A. O., Amit, E., & Ledgerwood, A. (2015). The effects of psychological distance on abstraction: Two meta-analyses. In.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security, 56*, 70-82. doi:http://dx.doi.org/10.1016/j.cose.2015.10.006

Sommestad, T., & Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. In *Security and Privacy Protection in Information Processing Systems* (pp. 257-271): Springer.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-Analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy, 9*(1), 26-46. doi:10.4018/IJISP.2015010102

Straub, D. W. (1989). Validating instruments in MIS research. *MIS quarterly*, 147-169.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 441-469.

Sue, V. M., & Ritter, L. A. (2007). *Conducting Online Surveys*. Los Angeles: SAGE Publications, Inc.

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology, 29*(3), 233-244.

Todorov, A., Goren, A., & Trope, Y. (2007). Probability as a psychological distance: Construal and preferences. *Journal of Experimental Social Psychology, 43*(3), 473-482.

Trope, Y., & Liberman, N. (2003). Temporal construal. *Psychological review, 110*(3), 403.

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological review, 117*(2), 440.

Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of consumer psychology, 17*(2), 83-95.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *computers & security, 52*, 128-141.

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *computers & security, 29*(4), 476-486.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems*, *29*(4), 263-290. doi:10.2753/MIS0742-1222290410

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3–4), 190-198. doi:http://dx.doi.org.proxy.kennesaw.edu/10.1016/j.im.2012.04.002

Verizon. (2018). 2018 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

Wakslak, C. J., Trope, Y., Liberman, N., & Alony, R. (2006). Seeing the forest when entry is unlikely: probability and the mental representation of events. *Journal of Experimental Psychology: General, 135*(4), 641.

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems, 17*(3), 194-215.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM, 46*(8), 91-95.

Whitman, M. E. (2008). Security Policy. *Information Security: Policy, Processes, and Practices*, 123.

Whitman, M. E., & Mattord, H. J. (2012). *Hands-on information security lab manual*: Cengage Learning.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly, 37*(1), 1-20.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal, 28*(2), 266-293.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329-349.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Wu, Y., Stanton, B. F., Li, X., Galbraith, J., & Cole, M. L. (2005). Protection motivation theory and adolescent drug trafficking: relationship between health motivation and longitudinal risk involvement. *Journal of pediatric psychology, 30*(2), 127-137.

Zhou, K. Z., & Li, C. B. (2012). How knowledge affects radical innovation: Knowledge base, market knowledge acquisition, and internal knowledge sharing. *Strategic management journal, 33*(9), 1090-1102.

APPENDIX A

Scales of Measures

Protection Motivation

Items to measure protection motivation by Posey et al. (2015):

1. I am motivated to protect my information from its security threats.
2. My intentions to prevent my information security threats from being successful are high.
3. It is likely that I will engage in activities that protect my information and information systems from security threats.

Modified Protection Motivation Items

1. I am motivated to protect my information / information systems from security threats now.
2. It is likely that I will engage in activities that protect my information / information systems from security threats immediately.
3. I have high intentions to prevent security threats from being successful.
4. I predict that I will immediately protect my information / information systems from security threats.
5. I intend to promptly protect my information / information systems from information security threats.

Risk Propensity

Scale to measure risk propensity (Sitkin & Weingart, 1995):

Participants will be asked: “when you face a decision that affects you, how would you rate your tendency to (1 = very unlikely to 7 = very likely). . .

1. Choose more or less risky alternatives based on the assessment of others on whom you must rely
2. Choose more or less risky alternatives which rely upon analyses high in technical complexity
3. Choose more or less risky alternatives which could have a major impact on you
4. Initiate a strategic action which has the potential to backfire
5. Support a decision when I am aware that relevant analyses were done while missing several pieces of information

Comparative Analysis

The following instruments for threat and coping appraisals are adopted from Johnston and Warkentin (2010) will be used for comparative analysis to show different in impact between the traditional use of PMT in the context of information security and the newly created instrument for psychological process manipulations. The following items will be used to measure threat appraisal.

1. My computer is at risk for becoming infected with malware.
2. It is likely that my computer will become infected with malware.
3. It is possible that my computer will become infected with malware.

The following items will be used to measure coping appraisal:

1. Anti-malware software is easy to use.
2. Anti-malware software is convenient to use.
3. I am able to use anti-malware software without much effort.

All items were measured using 7-point Likert-type scales from 1 = strongly disagree to 7 = strongly agree.

APPENDIX B

Manipulation Scenarios

Group 1 Concrete Scenario

You are a College of Business university student. This is the last week of classes and finals are next week. You are currently enrolled in a capstone project class. All students must successfully complete this class in order to graduate. The deadline for the complete project submission is in two days.

Today you just learned about what happened to a close friend of yours who is also finishing the capstone project. Last night as your friend was doing some last-minute internet research, his / her computer was suddenly locked. A message on the computer told your friend to pay $2000.00 to unlock the computer. Without unlocking the computer, your friend is unlikely to be able to finish the project and graduate. You are in the middle of the same project with some internet research left to do.

The university utilizes its official email system and its secure learning portal to communicate mitigating actions and periodically directs students' attention to avoid various malicious security threats such as this one. The university suggests the following actions to protect oneself from this specific threat:

- Don't visit or download materials from untrusted websites
- Make sure your anti-malware/antivirus is up-to-date
- Backup critical files using cloud storage
- When suspicious view training videos or contact the university information security office for immediate help

Training is always available online in the university's website and in the designated IT training location across campus, or by phone using the university's security hotline.

Table 29 shows the indicators of the psychological distance dimensions presented in the concrete scenario.

Table 29: Psychological Distance Dimensions Presented in the Concrete Version of Scenario 1

Dimension	Scenario terms	Distance
Temporal	Events are current as indicated by: today, two days, and next week	Low
Spatial	Events are in the student's college and class	Low
Social	Events happening to the participant and participant's close friend	Low
Hypothetical	True event happened last night	Low

Group 1 Abstract Scenario

You are a College of Business university student. Next year you may plan to register for the capstone project class. It is optional for students to complete the capstone project class before graduation. If you choose to enroll, the deadline for the capstone project will be at the end of next year.

As you work on researching for your project, you remember having heard a story some time ago about something happened to a large corporation. What might have happened was that an employee of a company was doing some internet research when the company's computer that the employee was using was suddenly locked. A message on the computer told the employee that his/her company needed to pay money to unlock the computer. Without unlocking the computer, the company was unlikely to be able to gain access to files on this computer. Next year, if you are in the capstone project, you may need to do some internet search for the project work.

The university offers general guidelines to increase students' awareness about potential malicious software. The university does not communicate specific actions about information security threats that external companies may deal with, as this threat may not target students. The university suggests reading their monthly information security newsletter to be familiar with current information security events. The university relies on students to use their discretion when it comes to protecting themselves from security threats.

Table 30 shows the indicators of the psychological distance dimensions presented in the abstract scenario.

Table 30: Psychological Distance Dimensions Presented in the Abstract Version of Scenario 1

Dimension	Scenario terms	Distance
Temporal	Events are in the future or happened in the past: next year, long ago	High
Spatial	Events are in an organization somewhere else	High
Social	Events happening to random person (an employee in an organization)	High
Hypothetical	Maybe the event night have happened	High

Group 2 Concrete Scenario

You are a College of Business university student. Today, your close friend and classmate told you what just happened to him. This morning he received the following email:

> You are receiving this email because you have authorized the university payroll to pay you through direct deposit. Due to recent system update, your direct deposit routing and account numbers will need to be updated by Friday. Failure to do so will stop the direct deposit access. Any unprocessed payments will be deferred to the following pay cycle. For timely payments and successful direct deposit of your paycheck, please make sure your direct deposit information are updated immediately.
>
> To update your direct deposit information please click on the link below and verify account information.
>
> https://payroll.update-direct-deposite.edu
>
> Remember to save your current information once update is complete.
>
> Thank you.
>
> Payroll Team

He receives a paycheck every two weeks because he is a student worker at the college of business. As instructed, he followed the directions. Few hours later, he received a bank notification regarding an overdraft charge. When he inquired, he found out that his account was accessed this morning and his current balance is $0.00. The transaction timestamp shows that the activity took place soon after he updated the direct deposit information. Your friend was a phishing victim.

Typical phishing message always claim to be from a recognized source and ask to verify your information. It also contains a link to redirect the user to a specific website where they can collect the needed personal information. To protect against this type of scam, your organization created policies that prohibit the communication of any financial information via email. Your organization also provides an ongoing security awareness training that, among other things, explains how to detect such attack and discourages users from communicating sensitive personal or corporate information. Also your organization created a two-step verification where the organization will send you a code then this code will be used to get to the login page.

Table 31 shows the indicators of the psychological distance dimensions presented in the concrete version of scenario 2.

Table 31: Psychological Distance Dimensions Presented in the Concrete Version of Scenario 2

Dimension	Scenario terms	Distance
Temporal	Events are current as indicated by: today, this morning, and few hours later	Low
Spatial	Events are in the student's college and class	Low
Social	Events happening to the participant's close friend	Low
Hypothetical	True event happened this morning	Low

Group 2 Abstract Scenario

Last year you heard a story about a worker at a company who received an email regarding his/her payment authorization. The message informed the employee that their direct deposit information may need to be updated or a delay in payment may occur. The story was unclear whether there was an incident that followed. This could be a phishing attempt to collect private information. Although, this may never happen, once a year organizations send an email communication to encourage employees not to share their private information. To protect against phishing scams, users are discouraged from sharing their own sensitive information. Also companies may have policies and procedures to increase employee awareness of this threat.

Table 32 shows the indicators of the psychological distance dimensions presented in the abstract version of scenario 2.

Table 32: Psychological Distance Dimensions Presented in the Abstract Version of Scenario 2

Dimension	Scenario terms	Distance
Temporal	Events are in the future or happened in the past: several months ago	High
Spatial	Events are in an organization somewhere else	High
Social	Events happening to random person (an employee in an organization)	High
Hypothetical	Maybe the event will never happen	High

APPENDIX C

Instruments

Study One Instrument

Consent Form

You are invited to participate in a web-based online survey on information security. This is a research project being conducted by Ashraf Mady, for the doctoral dissertation at Kennesaw State University. It should take approximately 15 minutes to complete.

Participation

Your participation in this survey is voluntary. You may refuse to take part in the research or exit the survey at any time without penalty.

Benefits

You will receive course credit for participating in this research study. Randomly, 10 participants each will receive a $10 Starbucks gift card. Also, your responses may help us learn more about the human behavior side of information security.

Risks

The risk from participating in this survey is minimal risk. The probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life.

Confidentiality

Your survey answers will be sent to a link at Qualtrics.com where data will be stored in a password protected electronic format. Qualtrics does not collect any identifying information such as your name, email address, or IP address. Therefore, your responses will remain anonymous. No one will be able to identify you or your answers, and no one will know whether or not you participated in the study.

Contacts

If you have questions at any time about the study or the procedures, you may contact me via email at anm9230@students.kennesaw.edu or my research supervisor, Professor Saurabh Gupta via email at sgupta7@kennesaw.edu

Research at Kennesaw State University that involves human participants is carried out under the oversight of an Institutional Review Board. Questions or problems regarding these activities should be addressed to the Institutional Review Board, Kennesaw State University, 585 Cobb Avenue, KH3403, Kennesaw, GA 30144-5591, (470) 578-2268.

Please select your choice below. Selecting "Yes I agree to participate" indicates that

- ✓ You have read the above information
- ✓ You voluntarily agree to participate

Electronic Consent Selection:

- ○ Yes I agree to participate

○ No I do not agree to participate (if this response is selected you will automatically exit the survey)

Students who select “No I do not agree to participate” will immediately exit the survey. Students who select “Yes I agree to participate” will be directed to complete the survey below:

Gender

○ Male
○ Female
○ Other
○ Prefer not to disclose

Age

○ Under 18
○ 18 - 21
○ 22 - 30
○ 31 - 40
○ 41 - 50
○ Over 50

Academic Class

○ Freshman
○ Sophomore
○ Junior
○ Senior

Major

▼ please select major:

○ Accounting
○ Computer Science
○ Finance
○ Information Systems
○ Management
○ Marketing
○ Other

Describe your level of computer experience

- ○ Not at all Familiar
- ○ Slightly Familiar
- ○ Moderately Familiar
- ○ Extremely Familiar
- ○ Expert

Imagine that you have to make a tough decision that involves trade-offs such as money or opportunity. Please read the questions below and rate your tendency to choose a risky alternative.

I tend to choose a risky alternative...

	Never	Rarely	Sometimes	About half the time	Most of the time	Often	Always
based on the assessment of others.	○	○	○	○	○	○	○
that could have a major impact on me.	○	○	○	○	○	○	○
that has the potential to backfire.	○	○	○	○	○	○	○
even when aware that I am missing several pieces of information.	○	○	○	○	○	○	○

Group 1 Concrete Scenario

This study will randomly present two scenarios to you. Each scenario will describe, in a similar way, a specific situation. Please watch the scenario and imagine yourself in this scenario. Below is the script for the concrete scenario:

You are a College of Business university student. This is the last week of classes and finals are next week. You are currently enrolled in a capstone project class. All students must successfully complete this class in order to graduate. The deadline for the complete project submission is in two days.

Today you just learned about what happened to a close friend of yours who is also finishing the capstone project. Last night as your friend was doing some last-minute internet research, his / her computer was suddenly locked. A message on the computer told your friend to pay $2000.00 to unlock the computer. Without unlocking the computer, your friend is unlikely to be able to finish the project and graduate. You are in the middle of the same project with some internet research left to do.
The university utilizes its official email system and its secure learning portal to communicate mitigating actions and periodically directs students' attention to avoid various malicious security threats such as this one. The university suggests the following actions to protect oneself from this specific threat:

- Don't visit or download materials from untrusted websites
- Make sure your anti-malware/antivirus is up-to-date
- Backup critical files using cloud storage
- When suspicious view training videos or contact the university information security office for immediate help

Training is always available online in the university's website and in the designated IT training location across campus, or by phone using the university's security hotline.

Based on the above scenario, please answer the following questions:

I believe that the risk from malicious websites would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
immediate.	○	○	○	○	○	○	○
personal.	○	○	○	○	○	○	○
realistic.	○	○	○	○	○	○	○
distant.	○	○	○	○	○	○	○

I could imagine malicious websites attacks...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
happening now.	○	○	○	○	○	○	○
happening to me.	○	○	○	○	○	○	○
happening nearby.	○	○	○	○	○	○	○
actually happening.	○	○	○	○	○	○	○

I think the damage from malicious websites attacks would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
close to home.	○	○	○	○	○	○	○
personally relevant.	○	○	○	○	○	○	○
instantaneous.	○	○	○	○	○	○	○
hypothetical.	○	○	○	○	○	○	○

Please rate your perception of this scenario in terms of its degree of concreteness or abstractness

Extremely abstract

- ○ Abstract
- ○ Somewhat abstract
- ○ Neither concrete nor abstract
- ○ Somewhat concrete
- ○ Concrete
- ○ Extremely concrete

I believe that protecting myself from malicious websites attacks would...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
complicate my existing job tasks.	○	○	○	○	○	○	○
make my current job mentally demanding.	○	○	○	○	○	○	○
require a lot of thought and problem-solving.	○	○	○	○	○	○	○
make my existing job more challenging.	○	○	○	○	○	○	○
increase the difficulty of my current job.	○	○	○	○	○	○	○

I am motivated to protect my information from malicious websites attacks now.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

It is likely that I will engage in activities that protect my information from malicious websites attacks immediately.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree

- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I have high intentions to prevent malicious websites from being successful.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I predict that I will immediately protect my information from malicious websites.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I intend to promptly protect my information from malicious websites.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Comparative Analysis

My university’s information and information systems are vulnerable to security threats.

- Strongly disagree

○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

It is likely that an information security violation will occur to my university’s information and information systems.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

My university’s information and information systems are at risk from information security threats.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

Threats to the security of my university’s information and information systems are severe.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

In terms of information security violations, attacks on my university's information and information systems are severe.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I believe that threats to the security of my university's information and information systems are serious.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I believe that threats to the security of my university's information and information systems are significant.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

For me, taking information security precautions to protect my university's information and information systems is easy.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree

- Strongly agree

I have the necessary skills to protect my university's information and information systems from information security violations.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

My skills required to stop information security violations against my university's information and information systems are adequate.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Employee efforts to keep my university's information and information systems safe from information security threats are effective.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

The available measures that can be taken by employees to protect my university's information and information systems from security violations are effective.

- Strongly disagree
- Disagree
- Somewhat disagree

- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

The preventive measures available to me to stop people from accessing my university's information and information systems are adequate.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Group 1 Abstract Scenario

Please watch the scenario below that describes a certain situation. Imagine yourself in this scenario.
Below is the script for the scenario:

Please read the scenario below that describes a certain situation. Imagine yourself in this scenario. After reading this scenario, please respond to the following questions.

You are a College of Business university student. Next year you may plan to register for the capstone project class. It is optional for students to complete the capstone project class before graduation. If you choose to enroll, the deadline for the capstone project will be at the end of next year.

As you work on researching for your project, you remember having heard a story some time ago about something happened to a large corporation. What might have happened was that an employee of a company was doing some internet research when the company's computer that the employee was using was suddenly locked. A message on the computer told the employee that his/her company needed to pay money to unlock the computer. Without unlocking the computer, the company was unlikely to be able to gain access to files on this computer. Next year, if you are in the capstone project, you may need to do some internet search for the project work.

The university offers general guidelines to increase students' awareness about potential malicious software. The university does not communicate specific actions about information security threats that external companies may deal with, as this threat may not target students. The university suggests reading their monthly information security newsletter to be familiar with current information security events. The university relies on students to use their discretion when it comes to protecting themselves from security threats.

Based on the above scenario, please answer the following questions:

I believe that the risk from phishing would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
immediate.	○	○	○	○	○	○	○
personal.	○	○	○	○	○	○	○
realistic.	○	○	○	○	○	○	○
distant.	○	○	○	○	○	○	○

I could imagine phishing attacks...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
happening now.	○	○	○	○	○	○	○
happening to me.	○	○	○	○	○	○	○
happening nearby.	○	○	○	○	○	○	○
actually happening.	○	○	○	○	○	○	○

I think the damage from phishing attacks would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
close to home.	○	○	○	○	○	○	○
personally relevant.	○	○	○	○	○	○	○
instantaneous.	○	○	○	○	○	○	○
hypothetical.	○	○	○	○	○	○	○

Please rate your perception of this scenario in terms of its degree of concreteness or abstractness

- ○ Extremely abstract
- ○ Abstract
- ○ Somewhat abstract
- ○ Neither concrete nor abstract
- ○ Somewhat concrete
- ○ Concrete
- ○ Extremely concrete

I believe that protecting myself from phishing attacks would...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
complicate my existing job tasks.	○	○	○	○	○	○	○
make my current job mentally demanding.	○	○	○	○	○	○	○
require a lot of thought and problem-solving.	○	○	○	○	○	○	○

make my existing job more challenging.	○	○	○	○	○	○	○
increase the difficulty of my current job.	○	○	○	○	○	○	○

I am motivated to protect my information from phishing attacks now.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

It is likely that I will engage in activities that protect my information from phishing attacks immediately.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

I have high intentions to prevent phishing from being successful.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

I predict that I will immediately protect my information from phishing.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I intend to promptly protect my information from phishing.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Comparative Analysis

My university’s information and information systems are vulnerable to security threats.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

It is likely that an information security violation will occur to my university’s information and information systems.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

My university’s information and information systems are at risk from information security threats.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

Threats to the security of my university’s information and information systems are severe.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

In terms of information security violations, attacks on my university’s information and information systems are severe.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

I believe that threats to the security of my university’s information and information systems are serious.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree

○ Somewhat agree
○ Agree
○ Strongly agree

I believe that threats to the security of my university’s information and information systems are significant.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

For me, taking information security precautions to protect my university’s information and information systems is easy.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

I have the necessary skills to protect my university’s information and information systems from information security violations.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

My skills required to stop information security violations against my university’s information and information systems are adequate.

○ Strongly disagree

- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Employee efforts to keep my university’s information and information systems safe from information security threats are effective.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

The available measures that can be taken by employees to protect my university’s information and information systems from security violations are effective.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

The preventive measures available to me to stop people from accessing my university’s information and information systems are adequate.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

In your opinion, what was the difference between the two scenarios and did this impact your perception of the communicated threat?

____

____

____

____

____

Group 2 Abstract Scenario

This study will randomly present two scenarios to you. Each scenario will describe, in a similar way, a specific situation. Please watch the scenario and imagine yourself in this scenario. Below is the script for the abstract scenario:

Last year you heard a story about a worker at a company who received an email regarding his/her payment authorization. The message informed the employee that their direct deposit information may need to be updated or a delay in payment may occur. The story was unclear whether there was an incident that followed. This could be a phishing attempt to collect private information. Although, this may never happen, once a year organizations send an email communication to encourage employees not to share their private information. To protect against phishing scams, users are discouraged from sharing their own sensitive information. Also companies may have policies and procedures to increase employee awareness of this threat.

Based on the above scenario, please answer the following questions:

I believe that the risk from malicious websites would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
immediate.	○	○	○	○	○	○	○
personal.	○	○	○	○	○	○	○
realistic.	○	○	○	○	○	○	○

distant.	○	○	○	○	○	○	○

I could imagine malicious websites attacks...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
happening now.	○	○	○	○	○	○	○
happening to me.	○	○	○	○	○	○	○
happening nearby.	○	○	○	○	○	○	○
actually happening.	○	○	○	○	○	○	○

I think the damage from malicious websites attacks would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
close to home.	○	○	○	○	○	○	○
personally relevant.	○	○	○	○	○	○	○
instantaneous.	○	○	○	○	○	○	○
hypothetical.	○	○	○	○	○	○	○

Please rate your perception of this scenario in terms of its degree of concreteness or abstractness

- ○ Extremely abstract
- ○ Abstract
- ○ Somewhat abstract
- ○ Neither concrete nor abstract
- ○ Somewhat concrete

- ○ Concrete
- ○ Extremely concrete

I believe that protecting myself from malicious websites attacks would...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
complicate my existing job tasks.	○	○	○	○	○	○	○
make my current job mentally demanding.	○	○	○	○	○	○	○
require a lot of thought and problem-solving.	○	○	○	○	○	○	○
make my existing job more challenging.	○	○	○	○	○	○	○
increase the difficulty of my current job.	○	○	○	○	○	○	○

I am motivated to protect my information from malicious websites attacks now.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

It is likely that I will engage in activities that protect my information from malicious websites attacks immediately.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

I have high intentions to prevent malicious websites from being successful.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

I predict that I will immediately protect my information from malicious websites.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

I intend to promptly protect my information from malicious websites.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Comparative Analysis

My university’s information and information systems are vulnerable to security threats.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

It is likely that an information security violation will occur to my university’s information and information systems.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

My university’s information and information systems are at risk from information security threats.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Threats to the security of my university’s information and information systems are severe.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

In terms of information security violations, attacks on my university's information and information systems are severe.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I believe that threats to the security of my university's information and information systems are serious.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I believe that threats to the security of my university's information and information systems are significant.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

For me, taking information security precautions to protect my university's information and information systems is easy.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree

- Somewhat agree
- Agree
- Strongly agree

I have the necessary skills to protect my university’s information and information systems from information security violations.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

My skills required to stop information security violations against my university’s information and information systems are adequate.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Employee efforts to keep my university’s information and information systems safe from information security threats are effective.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

The available measures that can be taken by employees to protect my university’s information and information systems from security violations are effective.

- Strongly disagree

- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

The preventive measures available to me to stop people from accessing my university's information and information systems are adequate.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Group 2 Concrete Scenario

Please watch the scenario below that describes a certain situation. Imagine yourself in this scenario. Below is the script for the concrete scenario:

You are a College of Business university student. Today, your close friend and classmate told you what just happened to him. This morning he received the following email:

You are receiving this email because you have authorized the university payroll to pay you through direct deposit. Due to recent system update, your direct deposit routing and account numbers will need to be updated by Friday. Failure to do so will stop the direct deposit access. Any unprocessed payments will be deferred to the following pay cycle. For timely payments and successful direct deposit of your paycheck, please make sure your direct deposit information are updated immediately. To update your direct deposit information please click on the link below and verify account information. https://payroll.update-direct-deposite.edu

Remember to save your current information once update is complete.

Thank you.

Payroll Team

He receives a paycheck every two weeks because he is a student worker at the college of business. As instructed, he followed the directions. Few hours later, he received a bank notification regarding an overdraft charge. When he inquired, he found out that his account was accessed this morning and his current balance is $0.00. The transaction timestamp shows that the activity took place soon after he updated the direct deposit information. Your friend was a phishing victim.

Typical phishing message always claim to be from a recognized source and ask to verify your information. It also contains a link to redirect the user to a specific website where they can collect the needed personal information. To protect against this type of scam, your organization created policies that prohibit the communication of any financial information via email. Your organization also provides an ongoing security awareness training that, among other things, explains how to detect such attack and discourages users from communicating sensitive personal or corporate information. Also, your organization created a two-step verification where the organization will send you a code then this code will be used to get to the login page.

Based on the above scenario, please answer the following questions:

I believe that the risk from phishing would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
immediate.	○	○	○	○	○	○	○
personal.	○	○	○	○	○	○	○
realistic.	○	○	○	○	○	○	○
distant.	○	○	○	○	○	○	○

I could imagine phishing attacks...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree	Somewhat agree	Agree	Strongly agree

				nor disagree			
happening now.	○	○	○	○	○	○	○
happening to me.	○	○	○	○	○	○	○
happening nearby.	○	○	○	○	○	○	○
actually happening.	○	○	○	○	○	○	○

I think the damage from phishing attacks would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
close to home.	○	○	○	○	○	○	○
personally relevant.	○	○	○	○	○	○	○
instantaneous.	○	○	○	○	○	○	○
hypothetical.	○	○	○	○	○	○	○

Please rate your perception of this scenario in terms of its degree of concreteness or abstractness

- ○ Extremely abstract
- ○ Abstract
- ○ Somewhat abstract
- ○ Neither concrete nor abstract
- ○ Somewhat concrete
- ○ Concrete
- ○ Extremely concrete

I believe that protecting myself from phishing attacks would...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree	Somewhat agree	Agree	Strongly agree

				nor disagree			
complicate my existing job tasks.	○	○	○	○	○	○	○
make my current job mentally demanding.	○	○	○	○	○	○	○
require a lot of thought and problem-solving.	○	○	○	○	○	○	○
make my existing job more challenging.	○	○	○	○	○	○	○
increase the difficulty of my current job.	○	○	○	○	○	○	○

I am motivated to protect my information from phishing attacks now.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

It is likely that I will engage in activities that protect my information from phishing attacks immediately.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree

- Strongly agree

I have high intentions to prevent phishing from being successful.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I predict that I will immediately protect my information from phishing.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I intend to promptly protect my information from phishing.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Comparative Analysis

My university’s information and information systems are vulnerable to security threats.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree

- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

It is likely that an information security violation will occur to my university's information and information systems.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

My university's information and information systems are at risk from information security threats.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Threats to the security of my university's information and information systems are severe.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

In terms of information security violations, attacks on my university's information and information systems are severe.

- ○ Strongly disagree

- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I believe that threats to the security of my university's information and information systems are serious.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I believe that threats to the security of my university's information and information systems are significant.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

For me, taking information security precautions to protect my university's information and information systems is easy.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I have the necessary skills to protect my university's information and information systems from information security violations.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

My skills required to stop information security violations against my university's information and information systems are adequate.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Employee efforts to keep my university's information and information systems safe from information security threats are effective.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

The available measures that can be taken by employees to protect my university's information and information systems from security violations are effective.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree

- Strongly agree

The preventive measures available to me to stop people from accessing my university’s information and information systems are adequate.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

In your opinion, what was the difference between the two scenarios and did this impact your perception of the communicated threat?

____

____

____

____

Study Two Instrument

Consent Form

You are invited to participate in a web-based online survey on information security. This is a research project being conducted by Ashraf Mady, for the doctoral dissertation at Kennesaw State University. It should take approximately 15 minutes to complete.

Participation

Your participation in this survey is voluntary. You may refuse to take part in the research or exit the survey at any time without penalty.

Benefits

Your responses may help us learn more about the human behavior side of information security.

Risks

The risk from participating in this survey is minimal risk. The probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life.

Confidentiality

Your survey answers will be sent to a link at Qualtrics.com where data will be stored in a password protected electronic format. Qualtrics does not collect any identifying information such as your name, email address, or IP address. Therefore, your responses will remain anonymous. No one will be able to identify you or your answers, and no one will know whether or not you participated in the study.

Contacts

If you have questions at any time about the study or the procedures, you may contact me via email at anm9230@students.kennesaw.edu or my research supervisor, Professor Saurabh Gupta via email at sgupta7@kennesaw.edu

Research at Kennesaw State University that involves human participants is carried out under the oversight of an Institutional Review Board. Questions or problems regarding these activities should be addressed to the Institutional Review Board, Kennesaw State University, 585 Cobb Avenue, KH3403, Kennesaw, GA 30144-5591, (470) 578-2268.

Please select your choice below. Selecting "Yes I agree to participate" indicates that

- ✓ You have read the above information
- ✓ You voluntarily agree to participate

Electronic Consent Selection:

- ○ Yes I agree to participate
- ○ No I do not agree to participate (if this response is selected you will automatically exit the survey)

Participants who select “No I do not agree to participate” will immediately exit the survey. Participants who select “Yes I agree to participate” will be directed to complete the survey below:

Gender

- Female
- Male
- Other
- Prefer not to disclose

Age

- Under 18
- 18 - 21
- 22 - 30
- 31 - 40
- 41 - 50
- Over 50

Education

- Less than high school
- High school graduate
- Some college
- 2 year degree
- 4 year degree
- Master/Professional degree
- Doctorate

Employment

- Employed full time
- Employed part time
- Unemployed
- Retired

What industry is the company you work for in?

- Business
- Technology
- Construction
- Art and Design
- Architecture
- Government
- Other

Years of professional experience with your current organization

- Under one year
- 1-5 years
- 6-10 years
- More than 10 years

What department do you work in?

- Information Systems/Technology
- Marketing/Advertising
- Finance
- Business Strategy
- Legal
- Sales
- Other

Describe your level of computer experience

- Not at all Familiar
- Slightly Familiar
- Moderately Familiar
- Extremely Familiar
- Expert

How often do you work with technology in your job? Technology such as Microsoft Office, Email, Salesforce, Cloud-bases platform?

- Never
- Sometimes
- About half the time
- Most of the time
- Always

Imagine that you have an opportunity that exposes you to a financial or a personal risk. Please rate your risk-taking tendency below.

I tend to choose a risky alternative...

	Never	Rarely	Sometimes	About half the time	Most of the time	Often	Always

based on the assessment of others.	○	○	○	○	○	○	○
that could have a major impact on me.	○	○	○	○	○	○	○
that has the potential to backfire.	○	○	○	○	○	○	○
even when aware that I am missing several pieces of information.	○	○	○	○	○	○	○

News reports suggest that organizations and their employees continue to face circumstances that threaten the security of information/information systems. Such circumstances may threaten information's confidentiality, integrity, and availability. Information security threats include phishing emails for unauthorized access to sensitive information, malicious software that can destroy critical data and suspicious websites that threaten data confidentiality.

Please pick a threat that you have heard about or have some experience with:

○ phishing emails
○ malicious software applications
○ suspicious websites

For each question below, please think of your organization's information security policies and training programs, then check the response that best characterizes how you feel about each statement when you face threats from [Insert User Selected Threat].

My organization's information security policies and/or training programs help me...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

acquire diversified and wide-ranging security knowledge.	○	○	○	○	○	○	○
accumulate knowledge of multiple security threats.	○	○	○	○	○	○	○
gain a variety of technical knowledge about mitigating security threats.	○	○	○	○	○	○	○

My organization's information security policies and/or training programs give me ___________________ [Insert User Selected Threat].

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
thorough understanding and experience regarding	○	○	○	○	○	○	○
in-depth knowledge about dealing with	○	○	○	○	○	○	○
specific technical skills to mitigate	○	○	○	○	○	○	○

My organization's information security policies and/or training programs allow me to be ___________________ in finding solutions for threats from [Insert User Selected Threat]

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
innovative	○	○	○	○	○	○	○
creative	○	○	○	○	○	○	○
experiential	○	○	○	○	○	○	○

I believe that the risk from [Insert User Selected Threat] would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
immediate.	○	○	○	○	○	○	○
personal.	○	○	○	○	○	○	○
realistic.	○	○	○	○	○	○	○
far away.	○	○	○	○	○	○	○

I could imagine [Insert User Selected Threat] attacks...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
happening now.	○	○	○	○	○	○	○
happening to me.	○	○	○	○	○	○	○
happening nearby.	○	○	○	○	○	○	○
actually happening.	○	○	○	○	○	○	○

I think the damage from [Insert User Selected Threat] would be...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
close to home.	○	○	○	○	○	○	○
personally relevant.	○	○	○	○	○	○	○
instantaneous.	○	○	○	○	○	○	○
speculative.	○	○	○	○	○	○	○

I believe that protecting myself from [Insert User Selected Threat] would...

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
complicate my existing job tasks.	○	○	○	○	○	○	○
make my current job mentally demanding.	○	○	○	○	○	○	○
require a lot of thought and problem-solving.	○	○	○	○	○	○	○

Solutions available to keep my organization’s information / information systems safe from [Insert User Selected Threat] are successful.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

The available measures that I can take to protect my organization’s information / information systems from [Insert User Selected Threat] are effective.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

The preventive measures available to me to stop [Insert User Selected Threat] threats are adequate.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I am motivated to protect my information / information systems from [Insert User Selected Threat] now.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

It is likely that I will engage in activities that protect my information / information systems from [Insert User Selected Threat] immediately.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I have high intentions to prevent [Insert User Selected Threat] from being successful.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

I predict that I will immediately protect my information / information systems from [Insert User Selected Threat].

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

I intend to promptly protect my information / information systems from [Insert User Selected Threat].

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

APPENDIX D

Study Two Descriptive Statistics

Table 33: Study Two Descriptive Statistics

Gender		
	Frequency	Percent
Female	165	75.3%
Male	54	24.7%
Total	219	100%
Age		
	Frequency	Percent
18-21	4	1.8%
22-30	45	20.5%
31-40	57	26%
41-50	59	26.9%
Over 50	54	24.7%
Total	219	100%
Education		
	Frequency	Percent
Less than high school	2	0.91%
High school graduate	25	11.42%
Some college	43	19.63%
2 year degree	22	10.05%
4 year degree	82	37.44%
Master/Professional degree	40	18.26%
Doctorate	5	2.28%
Total	219	100%
Professional Experience with Current Organization		
	Frequency	Percent
Under one year	14	6.39%
1-5 years	91	41.55%
6-10 years	37	16.89%
More than 10 years	77	35.16%
Total	219	100%
Computer Experience		
	Frequency	Percent
Slightly familiar	6	2.7%
Moderately familiar	73	33.3%
Extremely familiar	118	53.9%
Expert	22	10%
Total	219	100%
Technology Use in the Job		
	Frequency	Percent
About half the time	42	19.2%

Most of the time	80	36.5%
Always	97	44.3%
Total	219	100%
Industry Type		
Business	40	18.3%
Construction	5	2.3%
Art and Design	5	2.3%
Architecture	4	1.8%
Government	22	10%
Other	143	65.3%
Total	219	100%