12-15-2012

Expanding Protection Motivation Theory: The Role of Individual Experience in Information Security Policy Compliance

Leigh A (Leigh Ann) Mutchler

Expanding protection motivation theory: The role of individual experience in information security policy compliance

By

Leigh Ann Mutchler

A Dissertation
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
in Management Information Systems
in the Department of Management and Information Systems

Mississippi State, Mississippi

December 2012

Expanding protection motivation theory: The role of individual experience in information security policy compliance

By

Leigh Ann Mutchler

Approved:

Merrill Warkentin Professor of Management and Information Systems (Director of Dissertation)	Robert F. Otondo Associate Professor of Management and Information Systems (Committee Member)
Kent Marett Associate Professor of Management and Information Systems (Committee Member)	Robert E. Crossler Assistant Professor of Management and Information Systems (Committee Member)
Joe Sullivan Professor of Marketing, Quantitative Analysis, and Business Law (Committee Member)	Allen C. Johnston Committee Participant of Management and Information Systems (Committee Member)
Rebecca G. Long Associate Professor of Management and Information Systems (Graduate Coordinator)	Sharon L. Oswald Dean of the College of Business

Name: Leigh Ann Mutchler

Date of Degree: December 15, 2012

Institution: Mississippi State University

Major Field: Management Information Systems

Major Professor: Dr. Merrill Warkentin

Title of Study: Expanding protection motivation theory: The role of individual experience in information security policy compliance

Pages in Study: 171

Candidate for Degree of Doctor of Philosophy

The purpose of the present study is to make contributions to the area of behavioral information security in the field of Information Systems and to assist in the improved development of Information Security Policy instructional programs to increase the policy compliance of individuals. The role of an individual's experience in the context of information security behavior was explored through the lens of protection motivation theory. The practical foundation was provided by the framework of Security Education, Training, and Awareness (SETA) programs which are typically used by organizations within the United States to instruct employees regarding information security. A pilot study and primary study were conducted with separate data collections and analyses. Both existing and new measures were tested in the study which used a Modified Solomon Four Group Design to accommodate data collection via a web-based survey that included a two-treatment experimental component.

The primary contribution to academia proposed in this study was to expand the protection motivation theory by including direct and vicarious experience regarding both threats and responses to the threats. Clear definitions and valid and reliable reflective

measures for each of the four experience constructs were developed and are presented in this dissertation. Furthermore, the study demonstrated that all four forms of experience play an important part in the prediction of the primary constructs in the protection motivation model, and as such ultimately play an important part in the prediction of behavioral intent in the context of information security.

The primary contribution to practice was expected to be specifically related to the application of fear appeals within a SETA instructional framework. The contribution to practice made by this dissertation became instead the implications resulting from the strong performance of the experience constructs. Specifically, experience, both direct and vicarious, and with threats and with responses, are all important influences on individuals' behavioral choices regarding information security and should continue to be explored in this context.

DEDICATION

This dissertation is dedicated to my family. First, this dissertation could not have been completed without the support of my husband Eric and my children Norene and Evalina. They came along with me on this journey as I pursued my dream, accepting, without hesitation and without complaint, the changes in our lives that were necessary for the past four years to be a success. I also dedicate this dissertation to my siblings Sue, Beth, Jan, Don, and Kathryn, and especially to my parents, Calvin and Peggy. I will forever be appreciative of their encouragement and support throughout my life.

ACKNOWLEDGEMENTS

A sincere thank you goes to my committee members who taught me how to develop the skills I need to succeed as an academic. To Dr. Robert Otondo, Dr. Kent Marett, and Dr. Robert Crossler; your doors were always open to me, and I thank you for your time and guidance. To Dr. Joe Sullivan; you inspired me to always strive for the highest level of accuracy in my research, and I thank you for your willingness to share your vast knowledge of statistics. I also wish to offer my thanks to my outside committee member, Dr. Allen Johnston. Your MISQ publication, coauthored with Dr. Merrill Warkentin, was a large part of the inspiration for this dissertation, and I thank you for accepting my request for your input.

I offer a special thank you to my committee chair, Dr. Merrill Warkentin. You set a superior example for me as a researcher and teacher and I plan to repay you through my future successes. Your encouragement and the example you set for me as I progressed through my program was greatly appreciated and kept me moving forward to get to where I am today. I will always be grateful to you for your time and advice and for having had the opportunity to work with you. I look forward to a continued relationship with you as a fellow researcher, coauthor, and friend. Thank you.

Over the past four years, numerous other members of the faculty and staff at Mississippi State University have provided assistance and support to me as I endeavored to complete my studies and my dissertation project. In particular, I wish to thank the entire faculty of the Management and Information Systems Department in the College of

Business for the kind words and actions that encouraged me to continue moving forward in my program. I also want to thank Ms. Nadine Rosinski who was always helpful and available to me whenever I needed assistance of any kind. Last, I thank my fellow doctoral students in the Management Information Systems program; I am grateful to have known you and to have worked with you, and I look forward to continuing to develop our professional relationships and personal friendships as we each move on to various locations and postings in the future.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ADF = Asymptotic Distribution-free

AGFI = Adjusted Goodness of Fit

ANOVA = Analysis of Variance

AVE = Average Variance Extracted

Bartlett's = Bartlett's Test of Sphericity

BEH = Behavioral Intent

C.R. = Critical Ratio

CFA = Confirmatory Factor Analysis

CFI = Comparative Fit Index

D^2 = Mahalanobis Distance

DRE = Direct Response Experience

DT = Deterrence Theory

DTE = Direct Threat Experience

DV = Dependent variable

EFA = Exploratory Factor Analysis

EJIS = European Journal of Information Systems

GDT = General Deterrence Theory

GFI = Goodness of Fit

HICSS = Hawaii International Conference on System Science

HiSOC = High Social Influence

ICIS = International Conference on Information Systems

IS = Information Systems

ISJ = Information Systems Journal

ISP = Information Security Policies

ISR = Information Systems Research

ITL = Information Technology Laboratory

IV = Independent variable

JAIS = Journal of AIS

JMIS = Journal of MIS

KMO = Kaiser-Meyer-Olkin Measure of Sampling Adequacy

LoSOC = Low Social Influence

MI = Modification Indices

MISQ = MIS Quarterly

ML = Maximum Likelihood

MS4G = Modified Solomon Four Group

MSU = Mississippi State University

NFI = Normed Fit Index

NIST = US National Institute of Standards and Technology

PMT = Protection Motivation Theory

REF = Response Efficacy

RMR = Root Mean Square Residual

RMSEA = Root Mean Square Error of Approximation

RSC = Response Cost

S.E. = Standard Error

S4G = Solomon Four Group

SEF = Self-efficacy

SEM = Structured Equation Modeling

SETA = Security Education, Training, and Awareness

SMC = Squared Multiple Correlations

SOC = Social Influence

TPB = Theory of Planned Behavior

TRA = Theory of Reasoned Action

TSU = Threat Susceptibility

TSV = Threat Severity

VRE = Vicarious Response Experience

VTE = Vicarious Threat Experience

CHAPTER I

INTRODUCTION

As computing and telecommunications technologies continue to develop and improve, communication and collaboration supported by technology has increased resulting in the creation of massive amounts of information. Organizations have developed critical dependencies on these new information resources (Dhillon & Backhouse, 2000; Kankanhalli, Teo, Tan, & Wei, 2003), therefore appropriate management and protection of information is necessary throughout all stages of information creation, capture, storage, and sharing.

The management and protection of information is known as information security, broadly defined as the maintenance of the confidentiality, integrity, availability, and accountability of an organization's information assets (Anderson, 2003; Bishop, 2003; Siponen, Baskerville, & Heikka, 2006; Warkentin & Johnston, 2006, 2008). The information assets of an organization may be managed and secured through use of technical and behavioral controls, and each organization can meet their information security needs by balancing the use of controls with the potential risks to the information assets (Anderson, 2003).

Information security policies (ISP) state the security requirements of the organization and define the rules, processes, and procedures that are necessary to secure organizational information assets (Thomson & von Solms, 1998; Vroom & von Solms, 2004). The behavioral controls within the ISP include rules regarding employee

behaviors, and employees must comply with these rules to ensure the varying forms of information assets are appropriately protected (Siponen, 2000; Siponen & Iivari, 2006; Warkentin & Johnston, 2006; Warkentin, Johnston, & Shropshire, 2011). If employees are expected to comply with the ISP, they need to be made aware of the behavioral requirements and understand how to implement them. This need is commonly addressed through instructional programs that provide employees with awareness of information security and of the ISP (Thomson & von Solms, 1998).

ISP compliance-related issues continue to be cited as being among the most important issues in organizations (Bulgurcu, Cavusoglu, & Benbasat, 2010; Dodge, Carver, & Ferguson, 2007; Kaplan, 2010; Loveland & Lobel, 2010; Prince, 2009; Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008), and the human element has been identified as the weakest link in any security policy or procedure (Kaplan, 2010; Tsohou et al., 2008; Warkentin & Willison, 2009). ISP success hinges on securing the information assets which relies on compliance by individuals throughout the organization (Doherty & Fulford, 2005; Straub & Welke, 1998; Warkentin & Johnston, 2006). Organizations reliance on information assets is expected to increase, and as long as humans remain as a key element of the security of information assets, research in the area of ISP compliance will be an important and necessary area of study.

The purpose of the present study is twofold. First, the results of this work will make a contribution to the area of behavioral information security in the field of information systems (IS). Second, the results of this work will provide support to aid in improving the development of ISP instructional programs such that an increase in individual compliance with ISP may be achieved. These contributions will be achieved through the development and test of an expansion of the protection motivation theory

(PMT) for use in the context of ISP compliance. This chapter begins with an introduction to ISP compliance issues, followed by an overview of the behavioral methods being currently recommended to encourage individual ISP compliance. An introduction to the foundations of the present research, including a discussion of PMT, followed by a presentation of the research questions that are explored is next. The chapter concludes by detailing the organization of the remaining chapters of the study.

Information Security Policy Compliance Issues

Employee awareness of information security continues to be in the list of top security issues for organizations (Davis, 2011; Richardson, 2011). An annual survey of security professionals employed at organizations with at least 100 employees in various industries across the United States (Davis, 2010, 2011) found that 23% of the respondents identified employee awareness as one of the major security challenges they faced, ranking it as the fifth most important security issue. The respondents further reported that the security awareness programs required 12% of their time in 2011. Figures from the surveys for the previous two years indicated the time requirements have been steadily increasing, with the time requirement reported at 11% in 2010, up from 9% as reported in 2009. Even though awareness efforts are increasing, the effectiveness of employee awareness programs is decreasing with a reported 15% effectiveness rating in 2010 but dropping to 11% in 2011. Employee awareness programs were reported to be the least effective among other organizational security practices in both years, the common reason believed to be that a change is occurring in the types of threats being encountered.

In other survey results (Davis, 2010; Richardson, 2011), authorized users and employees moved to the top position as the greatest threats to breaches or espionage

above that of cyber criminals. The majority of the intrusion attacks in the past were merely irritants with intruders gaining access just long enough to cause havoc. Today, the more common attack comes from an intruder that gains access to the enterprise systems and remains inside longer, resulting in more severe consequences. This threat, labeled "advanced persistent threat," is typically launched by a more professional attacker. These intruders cannot be effectively handled by technology alone as has been the case in the past.

Many of the threats today utilize psychological rather than technological techniques (Davis, 2010). One of these types of threats is phishing, a form of deceptive communication based on social engineering where the goal is to trick individuals into revealing personal or sensitive information to the attacker (Wright, Chakraborty, Basoglu, & Marett, 2010; Wright & Marett, 2010). While malware attacks remain at the top of the list of information security concerns, phishing has seen such a high rate of success that the number of incidents of phishing attacks recently surpassed those due to malware (Davis, 2010).

The human element has always been a part of information security and ISP issues (Loch, Carr, & Warkentin, 1992; Straub & Welke, 1998), but today humans are even more often the primary target and their response to these threats is frequently the key to success or failure of these unauthorized access attempts. Security professionals have discovered they must adjust their response mechanisms to better fend off the attacks (Davis, 2010), which includes adjusting the methods of preparing individuals to handle the threats. Regardless of the type of instruction the employee has received, many security professionals feel that the typical individuals do not see the threats as severely as

they should, suggested by some to be due to a perception by individuals that information security does not have real or tangible threats (Chuvakin, 2010).

The newest threats causing the greatest concern today include those related to the use of mobile devices, social networking sites, and cloud computing (Davis, 2011; Loveland & Lobel, 2010; Schwartz, 2010). Mobile device threats are expected to be among the greatest of the threats in the future, with major increases in intrusions enabled by mobile applications being reported at 23% in 2010 rising to 33% in 2011 (Davis, 2011). The primary mobile device security concern is the loss or theft of a mobile device that contains sensitive information. Use of social networking sites raises several concerns and enables new vulnerabilities to information loss (DeZabala & Baich, 2010). The biggest concerns are that these sites may be compromised, may be used by attackers to gather sensitive information, or that employees may leak sensitive information on the sites (Davis, 2011). With cloud computing, the security concerns are typically related to the loss of direct control over the information, bringing up ISP enforcement and data recovery concerns (Loveland & Lobel, 2010).

Three of the oldest information security issues which continue to be among the most frequently cited and which persist in requiring a great deal of security resources are password management, malware attack avoidance, and data loss prevention (Davis, 2010, 2011; Richardson, 2011). All three of these issues rely on the behavior of individuals for security success. As such, individual behavior toward any of these three security issues -- data loss prevention, malware attack avoidance, and password cracking prevention -- are important compliance issues, and data loss prevention is the issue to be addressed in the present study.

Security Education, Training, and Awareness

The battle to protect information security is waged on two fronts; technical and behavioral. The threats against information security and the weapons used against these threats, therefore, include both technical and behavioral as well (Bulgurcu et al., 2010; Tsohou et al., 2008). Examples of technical controls include computer monitoring (Ariss, 2002), firewalls and intrusion detection systems (Cavusoglu, Raghunathan, & Cavusoglu, 2009), biometrics (Ballard, Lopresti, & Monrose, 2007), encryption (Boncella, 2002), secure software configurations and use of anti-malware software. Behavioral methods include the development and use of policies, processes, and procedures, the success of which all rely on the compliant behavior of individuals. These behavioral-based methods vary in format from one organization to the next, examples of which may include security education, training, and awareness (SETA) programs (D'Arcy, Hovav, & Galletta, 2009; Peltier, 2005; Wilson & Hash, 2003), acceptable use policies (Doherty, Anastasakis, & Fulford, 2011), deterrence programs (Straub & Welke, 1998), use of persuasive technologies (Forget, Chiasson, & Biddle, 2007). Regardless of the method used within an organization, employee ISP compliance is the common goal. The SETA program is one of the most widely applied behavioral controls (Siponen, 2000) and therefore the method on which the present research will focus.

The ISP awareness instruction in a typical SETA program includes basic instruction that provides enough information to the employees such that they are made aware of potential security issues that may be encountered during a typical work day along with the recommended responses to the issues (Peltier, 2005; Spitzner, 2011; Wilson & Hash, 2003). These ISP compliance awareness programs are developed with the goal of delivering the appropriate type and amount of information to employees so

that they will understand and follow the ISP and procedures, which ultimately will ensure the security of the organization's information assets. The typical process includes providing employees with initial awareness instruction, followed by periodic exposure to security policy statements and acceptable usage guidelines to act as reminders and to keep proper information security behaviors fresh in the minds of employees.

Through collaboration with industry and academia, the Information Technology Laboratory (ITL), a part of the US National Institute of Standards and Technology (NIST), develops security standards and guidelines for use in protecting all information systems other than those related to national security. While the focus of the NIST publications is toward requirements for computer systems used within the US Federal Government facilities, the publications are also good models that are used by organizations throughout the United States to guide development of their own organizational ISP (Wilson, de Zafra, Pitcher, Tressler, & Ippolito, 1998; Wilson & Hash, 2003).

The development of any awareness instruction program must to be guided by the specific requirements of the organization, and therefore all programs should be unique to a certain extent. With this in mind, the NIST publications provide guidance by presenting recommended criteria rather than specific content to assist in developing information security instructional programs for employees in an organization. The recommended criteria for the level of security instruction necessary is to determine an individual's security learning needs based on the organizational responsibilities held. Three role levels are recommended; awareness, training, and education (Crossler & Belanger, 2009; Peltier, 2005; Wilson et al., 1998). The first role level is the general individual who must be aware of ISP in order to comply with them. The second role

level is that of the manager or supervisor who needs more than simple awareness, as they must assist in making individuals in roles below them aware of ISP, and therefore should be made aware and also provided with training about ISP. Last is the role of the IS or security professional who must be made aware of ISP, be trained about ISP, and also be educated about ISP because they will be involved in the development and implementation of ISP procedures throughout the organization. It is generally agreed that the employees in this last role level require more in depth instruction and understanding regarding information security and ISP within an organization, but no such general agreement exists for employees within the first two role levels. For this reason the present study will not address the last role level and the education instruction, but will instead focus on the first two role levels and the appropriateness and effectiveness of the awareness and training forms of instruction.

The process of learning starts with being told about a "what" (awareness) and progresses to being informed of the "how" (training), and ending with details of the "why" (education). The individual role in the organization determines which level of capability is appropriate, and that role serves as a guide to the level of ISP knowledge needed as illustrated in Table 1. The first level of instruction is where individuals are told "what" in order that they become "aware" of ISP. The second level of instruction is where individuals are told "how" through some form of training so that they will be able to perform the required behaviors. The first level of instruction is directed toward the general individual which includes the majority of all employees in most organizations and believed to be those typically responsible for ISP breaches. Although the second level is typically directed toward employees in supervisory or management positions, the present research will perform an experiment to explore whether including a level of

training may prove to better prepare employees to comply with ISP over that of the awareness instruction alone.

Table 1 Three Levels of Information Security Instruction

	AWARENESS	TRAINING	EDUCATION
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Learning Objective:	Recognition and Retention	Skill	Understanding
Example Teaching Method:	Media - Videos - Newsletters - Posters	Practical Instruction - Lecture and/or demo - Case study - Hands-on practice	Theoretical Instruction - Seminar and discussion - Reading and study - Research
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving, i.e., Recognition and Resolution (apply learning)	Essay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Adapted from Wilson et al. (1998)

Awareness may be defined as having knowledge of the existence of or as a familiarity with a security issue. Since ISP awareness is recommended for all employees, and employees may be quite varied in terms of education and background, the awareness instruction should be at a level that is appropriate for equal understanding; therefore it tends to focus on the most basic concepts. Recommendations for the transfer of the ISP knowledge and development of the familiarity may be to have the individual simply read a policy manual or attend a seminar or workshop where the general concepts are provided (Wilson et al., 1998). Other recommendations suggest the initial awareness instruction may be more effective if presented via a video presentation (Peltier, 2005), particularly one that uses computer-generated characters so as not to offend viewers with any

suggestion of race or ethnicity of the characters in the video (Spitzner, 2011). These recommended methods of awareness instruction are merely forms of persuasion with the goal being to persuade employees' to comply with the ISP. Recommendations for appropriate follow-up reminders vary and may be in the form of posters, flyers, screensavers, or other printed (non-video) media. Monthly or quarterly newsletters and/or "lunch-and-learn" sessions may also be effective, notifications of both of which may be disseminated via email (Spitzner, 2011). These follow-up methods are also merely forms of persuasion directed towards employee ISP compliance.

Most organizations heed the recommendation to adopt a SETA program and conduct employee awareness instruction (Anderson & Choobineh, 2008), although most neglect to expand their program beyond the basic guidelines provided by NIST (Crossler & Belanger, 2009). We continue to see reports indicating high employee noncompliance (Johnston & Hale, 2009) which may be a reflection of the non-organizational-specific SETA programs being implemented. Along with viruses, employee theft, fraud, or mischief, human error is among the most frequently cited security risk reported by organizations (Doherty & Fulford, 2005), another indication many of the SETA programs may be ineffective.

Mirroring the information security concerns of industry, the extant literature on ISP compliance research also includes a broad range of both technical and behavioral information security solution studies (Bulgurcu et al., 2010). Those works concerned with behavioral issues focus on attempting to understand or influence attitudes, change behaviors, or otherwise encourage individual compliance with ISP (D'Arcy et al., 2009; Siponen, Pahnila, & Mahmood, 2010; Spurling, 1995; Thomson & von Solms, 1998). Empirical behavioral studies have found employee carelessness (Siponen et al., 2010),

employee moral reasoning (Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009), employee self-efficacy (Rhee, Kim, & Ryu, 2009), or social learning and policy compliance efficacy (Warkentin et al., 2011) as possible influences of individual ISP compliance. Other studies have focused on SETA or other similar programs and their development, proposing improvements such as use of computer-based educational tools (Furnell, Gennatou, & Dowland, 2002), testing the program's effectiveness (Dodge et al., 2007), using persuasion (Forget et al., 2007), or proposing best practices (Kolb & Abdullah, 2009; Peltier, 2005; Thomson & von Solms, 1998). It has also been suggested that to create more successful awareness programs, security professionals should think more like marketers than teachers (Spitzner, 2011), should "sell" the security program to the individual (Peltier, 2005), or should incorporate journalistic techniques such as presenting the instruction like a news magazine television program with outside experts delivering the awareness instruction (Peltier, 2005; Spitzner, 2011).

A recent proposal published in IS literature and regarding ISP employee awareness suggests the reason for the high level of program failures is due to the lack of 1) a clear definition of information security instruction, and 2) theoretical support for information security program development (Karjalainen & Siponen, 2011). Within this particular argument, the researchers point out that information security threats often possess an intangible quality, resulting in subjective perceptions of information security threats and responses to the threats. Information itself, the very asset with which information security mechanisms are charged to protect, is highly intangible. This intangible nature contributes to an unreal perception of information security by individuals (Chuvakin, 2010); therefore, it is understandable that individuals may find information security difficult to relate to, to accept, or to perceive as important enough

for them to comply with ISP. Furthermore, the researchers suggest that due to the subjective nature of information security, use of persuasive messages is the more appropriate method to implement for ISP awareness instruction (Karjalainen & Siponen, 2011). The present study proposes to further explore the use of persuasive messages in the context of individual ISP compliance.

Introduction to the Foundations of the Study

It is not feasible to train all employees to be fully knowledgeable of all information security issues, therefore security instruction programs typically focus on making individuals aware of information security threats and responses through their ISP with the expectation that this awareness will result in ISP compliance. The various programs do not always work well, as is evident from the abundance and variety of research being performed to improve them (Crossler & Belanger, 2009; D'Arcy et al., 2009; Doherty et al., 2011; Karjalainen & Siponen, 2011). It has been proposed that awareness instruction should focus on persuasive messages to convince individuals to comply with security policies and behave in a secure manner (Karjalainen & Siponen, 2011). This line of thought will be used in the present research as the use of fear appeal persuasive messages is explored within the framework of the protection motivation theory (PMT).

Theoretical Foundations

Persuasive messages and their effects on individuals' attitudes, behaviors, and decision-making have been the focus of numerous studies by researchers in varying disciplines. A fear appeal is one particular type of persuasive message first studied in the 1950s (Janis & Feshbach, 1953, 1954) and since then more commonly found in the field

of communications (Witte, 1992), healthcare (Kline & Mattson, 2000), public safety (Lewis, Watson, Tay, & White, 2007), marketing (Dillard & Anderson, 2004), and most recently in the field of IS regarding information security (Anderson & Agarwal, 2010; Herath & Rao, 2009; Johnston & Warkentin, 2010). Fear appeals incorporate a level of fear or concern about an event as the key factor in a message to persuade individuals to act in a manner that is believed to be for their own good, for the good of society, or in the case of information security, for the protection of individual and organizational information assets. Proposed as a way to explain the effects of fear appeals on attitude change, the protection motivation theory (PMT) (Rogers, 1975) states that an effective fear appeal must include three variables, all of which must be perceived and understood by the individual for the communication to be successful. First, the message must include information about a bad event or threat that is relevant at some level to an individual. Next, the message must include an indication of the likelihood the event or threat will occur assuming nothing is done to prevent it. Last, information regarding how the individual may avoid or respond to the potential bad event or threat and how likely and effective the response will be at combatting the event must be included in the message (Rogers, 1975). Subsequent studies found evidence that self-efficacy interacted with other PMT variables and was a strong predictor of behaviors; therefore PMT was revised to include self-efficacy as a fourth variable (Maddux & Rogers, 1983). Once an individual has been exposed to the fear appeal, they must recognize and assess the threat severity. Assuming individuals perceive the event is a threat, they proceed to assess their susceptibility to the threat, followed by an analysis of the efficacy of the recommended response, and their self-efficacy to perform the response. The individual's perception of the level of threat severity, threat susceptibility, response efficacy, and self-efficacy will

result in a form of protection motivation, which ideally is the attitude or behavior change that the persuasive message intended (Maddux & Rogers, 1983; Rogers, 1975).

While studies using PMT as a theoretical foundation are becoming more common at IS conferences and journals (Anderson & Agarwal, 2010; Crossler, 2010; Johnston & Warkentin, 2010; Woon, Tan, & Low, 2005), the IS discipline is still only in the beginning stages of exploring the theory. Works to date that use PMT in the specific area of ISP compliance are reporting findings that suggest PMT holds great promise towards explaining individual information security behaviors. Furthermore, across these same studies the application of PMT varies and the findings being reported are inconsistent; therefore continuing to build a stream of research in this area is justified and necessary. The present study proposes to test an expanded PMT model which will contribute to the research stream and fill a gap found in the literature.

Research Questions

The PMT process model shown in Figure 1, adapted from Floyd, Prentice-Dunn, and Rogers (2000), illustrates that verbal persuasion (typically a fear appeal) is a source of information that, when received by an individual, will be processed through two cognitive mediating processes (threat appraisal and coping appraisal). The threat appraisal and coping appraisal will lead to protection motivation behaviors by the individual. A review of the PMT literature published in IS journals in the context of ISP compliance behavioral studies revealed that the influences of experience on the cognitive mediating processes, both observational learning and prior experience as shown in Figure 1, have yet to be fully explored; therefore, the present study proposes to fill this gap in the literature. Furthermore, because an individual may possess experience with

the threat as well as with the response, and both may influence the cognitive mediating processes, this dissertation will include measures of an individual's vicarious experience (observational learning) with the threat and with the response, and direct experience (prior experience) with the threat and with the response.

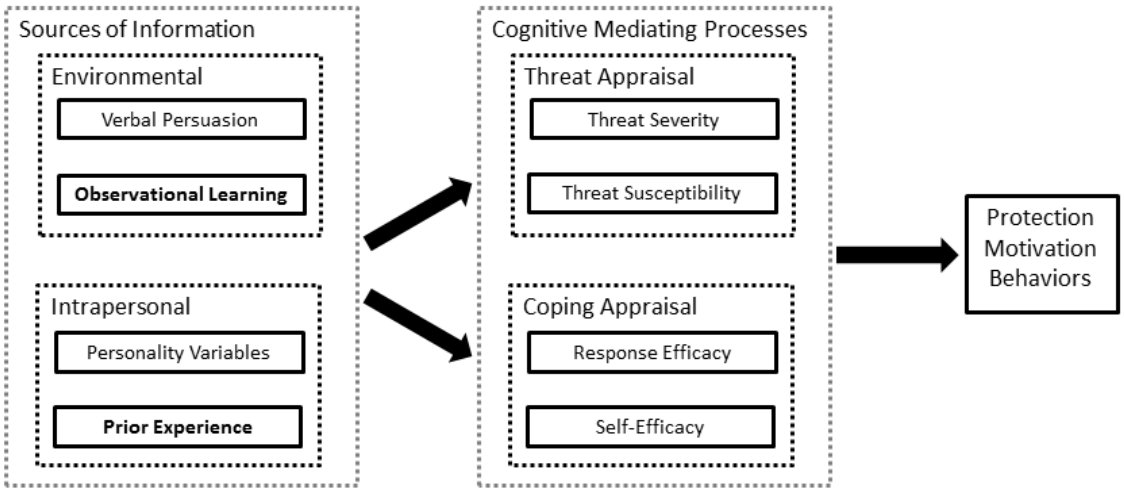

Figure 1 Protection Motivation Process Model (adapted from Floyd et al., 2000)

The expected contribution of this study is to add to the IS literature which seeks to understand individual information security behaviors and which in turn supports development of ISP instruction awareness programs such that an increase in employee compliance with ISP may be achieved. A thorough study with generalizable findings relevant to both academics and practitioners is desired; therefore, the present study performed an experiment, detailed in Chapter III, where an information security threat and response pair was explored through the use of a fear appeal (ISP awareness) and response instruction (ISP training). The research questions that were explored include:

RQ1: What role does an individual's past experience with an information security threat play in the individual's ISP compliance behavioral intent?

RQ2: What role does an individual's past experience with performing an information security response play in the individual's ISP compliance behavioral intent?

RQ3: Will use of response training with a fear appeal more likely result in individuals acting in a secure manner than with use of a fear appeal alone?

Organization of the Study

The organization of the present study begins with a literature review, model development, and hypotheses development in Chapter II. The research method is presented in Chapter III, and Chapter IV presents the results of the study. Chapter V concludes the study with a discussion of the findings and a presentation of the conclusions, limitations, and future implications. A copy of the survey invitations are in Appendix A and a copy of the data collection instrument is in Appendix B.

CHAPTER II

LITERATURE REVIEW, MODEL, AND HYPOTHESES

The purpose of the present study is to contribute to the information security literature and to information security policy (ISP) awareness programs through the development and test of an expansion of the protection motivation theory (PMT). This chapter begins with a review of the relevant extant literature, continues with a description of the model development, and concludes with the hypotheses to be tested.

Literature Review

Protection Motivation Theory

Persuasive messages about bad events or threats that are relevant at some level to an individual have been found to be influential in the behavior choices made by humans. PMT was developed by Rogers (1975) to provide a theoretical basis for multiple studies that had examined the use of fear appeals to persuade individuals to behave in a more health-conscious manner. Rogers noted that these earlier studies reported that stronger fear appeals in messages led to greater success in persuading individuals to be interested in the message, to perceive the threat as serious and concerning, to believe the threat should be avoided (Janis & Feshbach, 1953).

Originally, PMT stated that a fear appeal communication must provide the individual with information about a serious threat, inform them that a high probability of the threat occurring existed, and recommend an effective response to the threat in order to

encourage behavior by the individual to protect themselves from harm (Rogers, 1975). A revision to the original version included the necessary and theoretically supported addition of a self-efficacy component within the coping appraisal process (Maddux & Rogers, 1983). The cognitive processes of appraisals of the threat and of coping with the threat are performed by the individual and which result in the motivation to either positively or negatively cope with the threat (Floyd et al., 2000; Rogers, 1975).

Positive or adaptive coping is when the individual accepts the recommended response and positively copes with the threat, which is typically the intended outcome of a fear appeal. Along with the assessment of the response efficacy and the individual's self-efficacy to perform the response, the cost of performing the response was also found to play an important role in the coping appraisal (Floyd et al., 2000). These costs could be most any type of cost, including intangible costs such as effort, or tangible costs such as money. As long as the level of severity of the threat does not outweigh the individual's perception of the effectiveness of the recommended response or their ability to perform the response, the chance of achieving the intended outcome of the appeal is good (McGrath, 1995; Witte, 1992).

Negative or maladaptive coping may occur when the threat severity and coping ability are not properly balanced, for example when a strong threat is combined with a low coping ability. In this instance, the individual may react negatively to the fear appeal which may be exhibited by either avoiding the message, ignoring or choosing not to think about the threat, or in worst cases by reactance, a behavior sometimes called the "boomerang effect" where the individual chooses to behave in a completely opposite manner than that intended by the persuasive message (Lindsey, 2005; Roser & Thompson, 1995; Witte, 1992). Reactance theory may hold the answer to this

boomerang behavior, proposing that it may be caused by individuals perceiving that their freedom to behave as they choose or their ability to engage in certain behaviors whenever they wish is threatened (Lee, Lee, & Sanford, 2010). Therefore, if a fear appeal is to be used in an ISP awareness program, care must be taken to frame the appeal in such a way that threat severity and coping ability are balanced, but also such that the employees do not feel that complying with ISP will restrict their behavioral freedom.

Two PMT meta-analyses conducted to synthesize the PMT literature in the areas of health promotion and prevention (Floyd et al., 2000; Milne, Sheeran, & Orbell, 2000) are commonly cited in PMT research performed in the years since the two works were published. Both works reported that relationships between the coping appraisal and threat appraisal independent variables and the intention or behavior dependent variables were found in all the works reviewed. The coping variables consistently exhibited slightly stronger relationships than the threat variables. The coping variables were also found to have stronger relationships with behaviors when the target behavior was to stop an existing rather than start a new behavior. An individual's age was found to be positively related to coping behaviors, and self-efficacy and response efficacy relationships with behaviors were found to be the most stable relationships within PMT over time (Floyd et al., 2000).

Another discipline where persuasive messages have been utilized is that of public safety (Algie & Rossiter, 2010; Lewis et al., 2007). Within this discipline, research in the specific area of road safety has relied on the utilization of fear appeals for many years. Graphic images of the aftermath of a road accident caused by an individual driving under the influence or at a speed above the posted limit have been used to shock the public into obeying the law to prevent accidents of a similar nature. Evidence has been found

indicating that the key to achieving behavioral changes through the use of fear appeals in this context requires a focus on the individuals' perceptions of threat susceptibility and response efficacy (Lewis et al., 2007). Specifically, without feeling that a threat is real and possible, individual persuasion is unlikely to be successful. Without a recommended response that individuals perceive will work, the boomerang effect may be experienced, and individuals may respond by exhibiting behavior opposite from that which was intended by the message.

Plagiarism, a persistent problem in academia, has recently been exacerbated by the ease of access to information via the Internet. In an interesting and novel use of PMT, a study framed plagiarism as a threat to the integrity of academics, and presented anti-plagiarism software use as the response (Lee, 2011). While all variables within the threat and response appraisals were significant indicators of faculty members' software adoption intent, the threat appraisal variables were found to be the strongest indicators. Self-efficacy, response cost, and social influence were found to be insignificant. Response efficacy, however, was significant, an indication that the capability of the software was most important to the faculty.

In the field of information systems, the studies conducted to date involving fear appeals and PMT have produced successful and interesting results, suggesting there is a good fit of the theory within the context of information security. All the components for a PMT study exist; information security threats abound and their numbers and forms are increasing as we all continue to integrate technology and information systems throughout our personal and professional lives. These threats may affect most anyone, can cause great harm, and are becoming more likely to occur. Luckily, responses are available, typically work well, and are not usually difficult to perform. Information security

research with PMT as its theoretical foundation appears to be a fertile area of study. However, those studies performed to date have varying and inconsistent findings.

As with other disciplines, the threat and the response must also be balanced in the context of individual ISP compliance. The fear appeal may "scare" employees just enough to increase behavioral intent to comply, and as long as the ISP and procedures are perceived as effective and they believe they are able to perform them, they may follow through with the intended behavior. A recent study successfully used fear appeals in this way to increase the behavioral intent of individuals to use anti-spam software (Johnston & Warkentin, 2010). Awareness programs in general could benefit as well if employees are not only made aware of secure behavioral responses to threats, but also informed of the effectiveness of the recommended responses and provided assistance to improve their self-efficacy in performing the recommended responses. By including response training, employees may be better prepared to cope with information security threats (LaRose, Rifon, & Enbody, 2008).

In the 1980s and 1990s most employees relied on the organization for their computing experiences and therefore their ISP instruction as well. Exposure to information security threats and responses to the threats was almost solely through organization's instructional programs such as SETA. Today, however, three primary differences exist. First, the number of employees with access to computing equipment outside the workplace is now greater than the number of those without (Anderson & Agarwal, 2010). Next, organizations may choose to use a distributed rather than centralized security governance (Warkentin & Johnston, 2006). And last, an increasing number of employees are performing some or all of their organizational duties from home offices (Reuteman, 2011). These differences mean that when employees are

exposed to information security threats, the determination regarding responses may be self-directed. Therefore, a better understanding of individual security behavior is needed beyond as well as within the workplace.

Researchers have applied PMT to several specific information security contexts such as employee ISP compliance (Herath & Rao, 2009; Ifinedo, 2012; Pahnila, Siponen, & Mahmood, 2007; Vance, Siponen, & Pahnila, 2009), secure computing practices (Anderson & Agarwal, 2010; Ng, Kankanhalli, & Xu, 2009; Woon et al., 2005; Workman, Bommer, & Straub, 2008), use of anti-malware software (Garung, Luo, & Liao, 2009; Johnston & Warkentin, 2010; Lee & Larsen, 2009; Liang & Xue, 2010; Stafford & Poston, 2010), online safety (Banks, Onita, & Meservy, 2010; LaRose et al., 2008; LaRose, Rifon, Liu, & Lee, 2005; Marett, McNab, & Harris, 2011; Zhang & McDowell, 2009), and data backup (Crossler, 2010; Malimage & Warkentin, 2010). The findings of the research in these varying contexts will contribute to inform the development of ISP and ISP compliance instructional programs.

Employee compliance with ISP is critical to ensure the protection of information system assets. The findings of studies exploring individual behavior toward ISP compliance have been mixed. In one study, self-efficacy, response efficacy, threat vulnerability, and subjective norms were found to be significant influences for managers regardless of their information systems knowledge (Ifinedo, 2012). In another study, normative beliefs, threat severity and susceptibility were found to be significant indicators of compliance for employees, but self-efficacy and response efficacy were not. The strength of social influences in an organization setting suggests that managers and supervisors may be a critical component to encouraging employee ISP compliance (Pahnila et al., 2007).

An exploration into the factors that lead to home security behaviors found descriptive norms to be particularly important in influencing protective behaviors against a collective threat, while subjective norms were more influential against individual threats (Anderson & Agarwal, 2010). These findings indicate that social norms can influence individual information security behaviors even in the voluntary context of home computing. The findings also suggest that the subject of the threat may contribute to behavior as well, a notion also explored in the work environment through an examination of the relationship between employee organizational commitment and ISP compliance (Herath & Rao, 2009). To fully grasp the significance of ISP compliance, employees should better understand potential threats and responses, and should also understand their effects on the individual and the society as a whole.

Wireless home networks are becoming very common and as such represent a potential threat to individuals when not securely configured. For organizations with employees working from home, wireless home networks can also add to potential security threats to the organization. In a study of students with wireless home networks, self-efficacy was found to be most strongly related to the intent to enable secure features of a wireless network, and the severity of a threat was found to be more likely to encourage safe behavior than susceptibility to the threat (Woon et al., 2005).

The severity of the threat is often found to be a strong influence of secure behavior, and one study found that individuals will also implement a response with greater consistency when the threat is more severe, and for those perceived to have a higher probability, the consistency of the response will be even higher. Evidence was also found to indicate that threat severity assessment becomes less effective if individuals

experience numerous threat situations that are ultimately found to be false (Workman et al., 2008).

A study examining secure individual behaviors regarding emails that contain attachments (Ng et al., 2009) found that susceptibility and self-efficacy were strong indicators of secure behavior, while severity was not. Results also found that awareness instruction was not significant to encourage secure behavior.

Malware is a common information security threat typically addressed with anti-malware software use. A study involving the students, faculty, and staff of a large university found that social influence was the strongest indicator, followed by self-efficacy and response efficacy as indicators of secure behavioral intent. Other interesting results included finding perceived threat severity to be a significant predictor of self-efficacy and of response efficacy, two relationships not typically proposed in PMT research (Johnston & Warkentin, 2010). Another study produced similar findings, with threat severity, self-efficacy, and response efficacy being significant indicators of software use, with no significant contributions found from threat vulnerability and response costs (Garung et al., 2009).

Small and medium businesses (SMB) often lack information security expertise, and as such are similar to the home computing environment where information security behaviors are voluntary rather than mandated. The assumption cannot be made for all SMB, of course, as some do have information security resources available to them. This makes the SMB environment an important one for information security research, yet a shortage exists to date. The results of one study within the SMB environment (Lee & Larsen, 2009) included the existence of relationships between the threat and coping appraisal variables and behavioral intent. Perceptions of both threat severity and threat

susceptibility were the most important influences of the executives' intent to use anti-malware software, but the severity of the threat was the driving factor. Other interesting findings included executives' IS expertise and the SMB industry membership played influential roles as well. This suggests that the level of individual IS knowledge and the importance or depth of IS within organizational activities may be important factors worthy of additional exploration in all environments.

Several threats exist in the online environment, including social networking and password management. Posting personal information on social network websites is considered risky online behavior because the information may be used by others in ways unintended by the owner of the information. One study found the threat appraisal variables, particularly threat susceptibility, were strongly influential to encourage individuals to change this type of risky online behavior (Marett et al., 2011). Another study also found threat severity and susceptibility to be strong influences, and added social influence as being highly important (Banks et al., 2010). In the context of overall online safety behaviors of college students, self-efficacy and response efficacy were found to be the strongest factors related to secure behavioral intent (LaRose et al., 2008). In the case of password management for online account access, self-efficacy and response efficacy had strong positive relationships and response cost had a strong negative relationship with intent to implement strong passwords (Zhang & McDowell, 2009).

Any individual storing data is at risk for the threat of data loss. The most common response is to perform data backups. A study exploring data backup behavior within a population that varied from students to small business employees (Crossler, 2010) produced results indicating that self-efficacy and response efficacy were

significantly and positively related to behavior. Threat susceptibility and severity were also significantly related, but in the negative direction rather than positive. Response cost was found to be insignificant in this context. A similar study with a population consisting of faculty and staff at a major university found that threat severity, response efficacy and self-efficacy were strongly related to behavioral intent, but threat susceptibility was not (Malimage & Warkentin, 2010).

Research Model Development and Hypotheses

A recent study (Crossler, Johnston, Bélanger, & Warkentin, 2012) reviewed the extant literature addressing information security in the field of IS, focusing on those articles published through 2010 in the IS Senior Scholars basket of six journals ("Senior Scholars' Basket of Journals," 2011) which includes the *European Journal of Information Systems* (EJIS), *Information Systems Journal* (ISJ), *Information Systems Research* (ISR), *Journal of AIS* (JAIS), *Journal of MIS* (JMIS), and *MIS Quarterly* (MISQ), along with two IS conferences, International Conference on Information Systems (ICIS) and Hawaii International Conference on System Science (HICSS). The study discovered that only 22 works from those sources focused on behavioral information security. The various theoretical foundations used in the 22 articles included PMT as well as deterrence theory (DT), general deterrence theory (GDT), theory of reasoned action (TRA), and theory of planned behavior (TPB). As is often the case when a theory is found to be useful and begins to gain popularity in an area of study, the application of the theory and the constructs used will differ from one research work to the next. Of the 22 behavioral security studies found, 9 relied on PMT as a primary theory to provide a framework for the study and as expected, the application of the theory and the

constructs measured varied across the studies, and conflicting results were found (Crossler et al., 2012). The 9 articles are among those in the literature review section of this chapter, was included in the literature review section of the present study. The 9 articles were then used to produce a comprehensive information security-PMT model to serve as the basis for development of the research model. The following section discusses the development of the model.

Information Security-PMT Comprehensive Model

Due to the inclusion of other theories and the specific behavioral information security contexts addressed in the research works, the 9 articles reviewed included numerous and varying constructs. Those not theoretically linked to PMT were excluded from the comprehensive PMT model development. Referring to the most current PMT model which had been developed through meta-analysis of the studies performed in the research area of healthcare (see Figure 1) (Floyd et al., 2000), Table 2 was constructed and the PMT-related constructs found in the 9 articles reviewed were sorted into three main independent variable categories; sources of information, threat appraisal, and coping appraisal. The category of sources of information was further divided into direct and indirect sources of information based upon whether the construct was found to have a direct or indirect effect on the dependent variable (DV) in the work.

Table 2 PMT Constructs in Works Reviewed

Threat Appraisal	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Perceived Severity		x	x	x	x	x	x		x
Perceived Susceptibility				x		x	x		
Perceived Vulnerability		x			x				x
Perceived Probability			x						
Perceived Threat						x	x		
Concern Level			x						
Threat Concern	x								
Threat Appraisal								x	
Coping Appraisal	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Self-Efficacy	x	x	x	x	x	x	x		x
Response Efficacy		x	x	x	x	x	x		x
Perceived Citizen Efficacy	x								
Prevention Cost		x	x		x	x	x		x
Coping Appraisal								x	
Perceived Avoidability						x			
Sources of Info. (direct)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Descriptive Norm	x		x						
Subjective Norm	x		x						
Normative Beliefs								x	
Social Influence				x	x	x			
Organizational Commitment			x						
Psychological Ownership	x								
Vendor Support					x				
IT Budget					x				
Firm size					x				
Facilitating Conditions								x	
Information Quality								x	
Rewards								x	
Sanctions								x	
Habits								x	
Sources of Info. (indirect)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Social Influence						x			
Risk Tolerance						x			
Organizational Commitment			x						
Resource Availability			x						

A=Anderson and Agarwal (2010); B=Crossler (2010); C=Herath and Rao (2009); D=Johnston and Warkentin (2010); E=Lee and Larsen (2009); F=Liang and Xue (2009); G=Liang and Xue (2010); H=Pahnila et al. (2007); I=Woon et al. (2005)

Because the construct names and definitions in a research work are related to the context of the work and ultimately selected by the researcher, a closer examination of the constructs was next performed in order to develop a more parsimonious comprehensive Information Security-PMT model. The construct definitions and, if available, the measurement scales were compared in order to discover and reduce construct redundancies. As constructs were identified as redundant, they were grouped together under a single more general construct name, and the resulting summary of constructs is shown in Table 3. Using the most current PMT model (Figure 1) as a framework, the Information Security-PMT comprehensive model was developed and is shown in Figure 2. The next section will discuss the constructs in the Information Security-PMT Comprehensive model and the present study's research model development.

Table 3 Summarized PMT Constructs in Works Reviewed

Threat Appraisal	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Threat Susceptibility		x	x	x	x	x	x	x	x
Threat Severity		x	x	x	x	x	x	x	x
Concern	x		x						
Coping Appraisal	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Response Efficacy		x	x	x	x	x	x	x	x
Self-Efficacy	x	x	x	x	x	x	x	x	x
Response Cost		x	x		x	x	x		x
Citizen Efficacy	x								
Sources of Info. (direct)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Descriptive / Subjective Norm	x		x					x	
Social Influence				x	x	x			
Organizational Commitment			x						
Psychological Ownership	x								
Situation-specific Controls					x				
Facilitating Conditions					x			x	
Habits								x	
Sources of Info. (indirect)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Social Influence						x			
Risk Tolerance						x			
Organizational Commitment			x						
Resource Availability (facilitating conditions)			x						

A=Anderson and Agarwal (2010); B=Crossler (2010); C=Herath and Rao (2009); D=Johnston and Warkentin (2010); E=Lee and Larsen (2009); F=Liang and Xue (2009); G=Liang and Xue (2010); H=Pahnila et al. (2007); I=Woon et al. (2005)

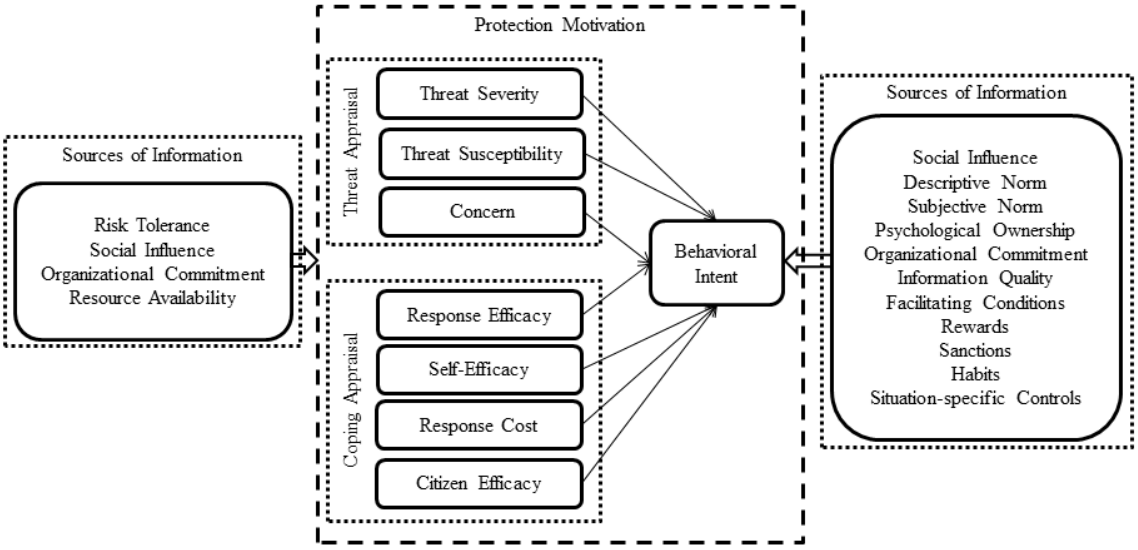

Figure 2 Information Security-PMT Comprehensive Model

Research Model

The common measures of threat appraisal within PMT include those of severity and susceptibility perceptions by the individual with regard to the persuasive message (a fear appeal). Similarly, common measures of coping appraisal within PMT include those of the individual's self- and response efficacy perceptions. All nine of the studies reviewed measured the individual constructs of threat severity and threat susceptibility, with the exception of two. Of the nine works reviewed, all but one included measurements of the constructs of response efficacy and all included self-efficacy measures. Therefore, the constructs for threat appraisal to be included in the research model are threat severity and threat susceptibility, and for coping appraisal are response efficacy and self-efficacy. A third coping appraisal measure often included is that of the individual's perception of the costs (monetary, time, inconvenience, or other opportunity costs) that an individual may perceive will be incurred by responding to the threat. A

majority, six of the nine works reviewed, included the construct of response cost, therefore the research model for the present study will as well.

In the PMT process model shown in Figure 1, prior experience is included as an interpersonal influence that may affect an individual's assessment of a threat, as well as an assessment of a response to cope with the threat. An experience construct can be found in information security studies but was not included in any of the nine PMT articles in the area of information security. Experience is explored in about half of the research conducted in the field of IS (Aguirre-Urreta & Marakas, 2008) where it is typically treated as either a time-based measure such as number of years in a particular job, a quantity measure such as the number of times a phenomenon occurs, or a measure of rank or category (Aguirre-Urreta & Marakas, 2008). Also, because an individual may possess either form of experience with a threat or with a response to a threat, both will be included in the model as well. Finally, although experience in the usage research literature has been shown to be a moderator of the determinants of behavioral intent (Venkatesh, Morris, Davis, & Davis, 2003), this is not the case for experience as explained by PMT. Therefore, in keeping with PMT the present study will include direct and vicarious response experience, and direct and vicarious threat experience as antecedents of the cognitive mediating processes leading to information security behavioral intent.

A large number of influences found in the nine articles reviewed were highly contextual and therefore are not considered for the present study which seeks to develop a more generalizable model. The normative beliefs variables that are found in several of the studies, however, are also included in key behavioral theories such as the theory of reasoned action (TRA) (Fishbein & Ajzen, 1975) and the theory of planned nehavior

(TPB) (Ajzen, 1985) and so are more generalizable across most contexts. Therefore, since this model is examining human behavioral intent, the normative belief construct of social influence will be included. Prior studies have found support for both direct and indirect influences of social influence on behavioral intent (Agarwal & Karahanna, 2000; Johnston & Warkentin, 2010) and therefore exploration of both will be performed in the present research model.

In summary, based on the literature review performed the independent constructs included in the present study are threat severity, threat susceptibility, response efficacy, self-efficacy, response cost, direct and vicarious response experience, and direct and vicarious threat experience. Additionally social influence is included as both an independent and a moderating variable. The following section discusses the hypotheses tested.

Hypotheses Development

An expanded predictive model based on PMT, a theory that explains how persuasive messages may be used to influence individual behavior, was explored. Social and behavioral research involves examining human behaviors under certain conditions in various contexts (McGrath, 1995). The present research examines human perceptions and human behavior and is therefore behavioral research. The actual behavior of an individual is frequently a challenge to measure. The theory of reasoned action (TRA) states intent precedes actual behavior (Fishbein & Ajzen, 1975) and that link is well established in IS research (Venkatesh et al., 2003). Behavioral intent often serves as a proxy for actual behavior in IS studies (Agarwal & Karahanna, 2000; D'Arcy et al., 2009). For these reasons and also because the majority of PMT research uses intent as a

dependent variable (Floyd et al., 2000), the dependent variable in the present research is behavioral intent.

The basis of PMT relies on the cognitive processes of threat appraisal and coping appraisal which affect the individual's protection motivation and which will result in adaptive or maladaptive coping with the threat. When presented with a persuasive message such as a fear appeal, the threat appraisal process assesses the strength and likelihood of the threat. Additionally the coping appraisal assesses the effectiveness and costs of the response and the individual's perception of their ability to successfully carry out the response. In this way, an individual's perceptions of the existence of a threat and of the likelihood of the threat occurring are related to the individual's acceptance of the persuasive message and therefore to their intent to behave in the manner recommended by the message.

Adaptive coping, typically the desired outcome of a persuasive message and the outcome on which the present study focuses, occurs when the threat severity is perceived as high, the threat is believed to be likely, the response is expected to be effective, the individual believes he or she is able to perform the response, and the costs of the response are not too high (Floyd et al., 2000; Maddux & Rogers, 1983; Witte, 1992). The first twenty-five of the hypotheses to be tested in the present study (see Figure 3) begin with expected positive relationships between the independent variables of threat severity, threat susceptibility, response efficacy, and self-efficacy, and the dependent variable behavioral intent. A negative relationship is expected between the independent variable response cost and the dependent variable behavioral intent.

H1a: Higher perceptions of threat severity will positively influence intent to perform the recommended secure behavior.

H2a: Higher perceptions of threat susceptibility will positively influence intent to perform the recommended secure behavior.

H3: Higher perceptions of response efficacy will positively influence intent to perform the recommended secure behavior.

H4: Higher perceptions of self-efficacy will positively influence intent to perform the recommended secure behavior.

H5: Higher perceptions of response cost will negatively influence intent to perform the recommended secure behavior.

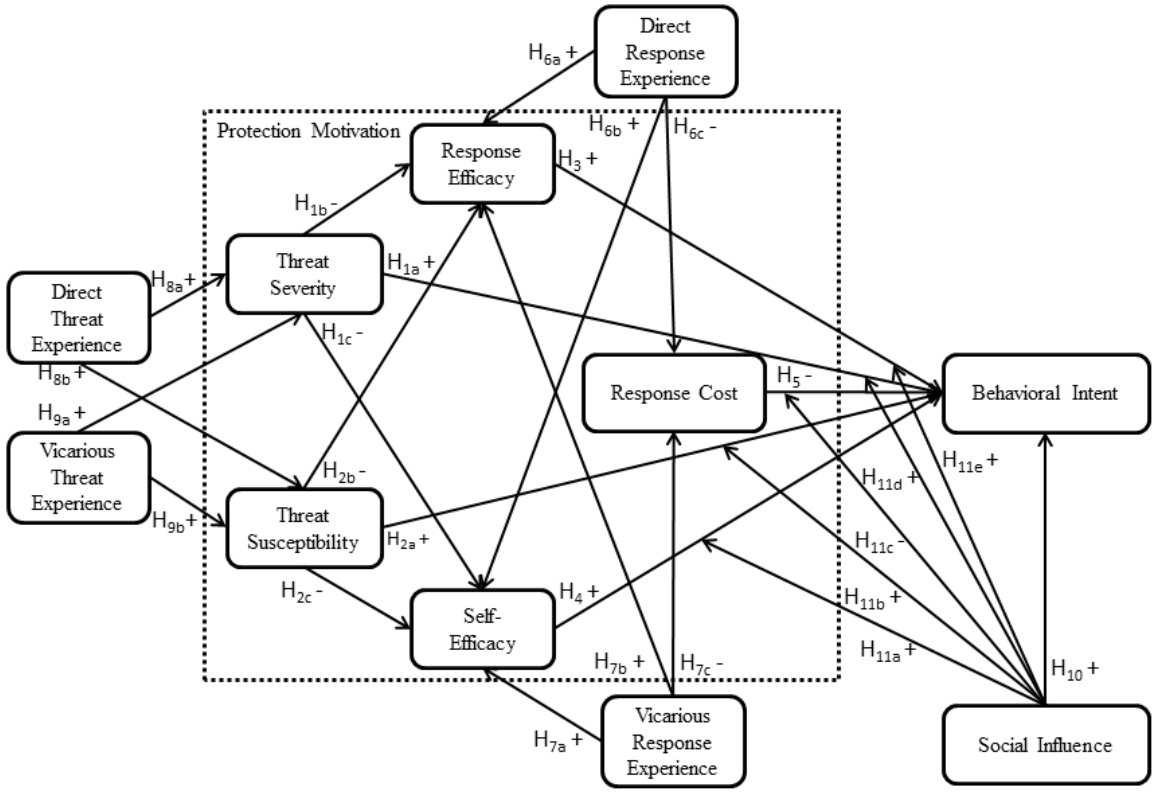

Figure 3 Prediction Model Illustrating Hypotheses H1a-H10

Much of the PMT research performed to date in the field of IS has neglected to explore relationships between the constructs of threat severity, threat susceptibility, response efficacy, and self-efficacy (Herath & Rao, 2009; Lee & Larsen, 2009; Pahnila et

al., 2007; Woon et al., 2005). Previous works in other fields, however, frequently examined and identified interactions between these constructs (Witte, 1992). Many assume a sequential path from the threat assessment to the coping assessment (Marett et al., 2011; Neuwirth, Dunwoody, & Griffin, 2000) and a logical argument can be made that the assessment of coping with a particular threat cannot be fully completed without first assessing the threat. This sequential arrangement suggests that either or both threat severity and threat susceptibility may influence either or both response efficacy and self-efficacy. Such relationships were tested byJohnston and Warkentin (2010) who found that hypotheses of negative relationships between threat susceptibility and response efficacy and between threat susceptibility and self-efficacy were not supported, but hypotheses of negative relationships between threat severity and response efficacy and threat severity and self-efficacy were supported. This leads to the next set of hypotheses to be tested (see Figure 3) and which will include the same negative relationship predictions.

H1b: Higher perceptions of threat severity will negatively influence response efficacy.

H1c: Higher perceptions of threat severity will negatively influence self-efficacy.

H2b: Higher perceptions of threat susceptibility will negatively influence response efficacy.

H2c: Higher perceptions of threat susceptibility will negatively influence self-efficacy.

Two forms of experience, direct and vicarious, are included in the PMT process model (Figure 1) as potential influences on the cognitive processes of threat appraisal and coping appraisal. Some form of experience measure has been included in a high percentage of all prior empirical IS research (Aguirre-Urreta & Marakas, 2008) and has been found to be important in information technology acceptance and use (Venkatesh et

al., 2003). The experience construct has been found to be an influence on behaviors, attitudes, and beliefs (Taylor & Todd, 1995), to aid in the development of self-efficacy (Bandura, 1977; Gist & Mitchell, 1992), is considered a dimension of competence and a contributor to tacit knowledge (Bassellier, Benbasat, & Reich, 2003), to reduce uncertainty enabling better decision making and assessments of problems (Sherwood & Covin, 2008), and to affect trust (Gefen, 2000). Based on this evidence from prior studies, experience is predicted to influence response efficacy, self-efficacy, response cost, threat severity, and threat susceptibility, and the following set of hypotheses shown in Figure 3 will be tested in the present study.

H6a: Higher levels of direct response experience will positively influence response efficacy.

H7b: Higher levels of vicarious response experience will positively influence response efficacy.

H6b: Higher levels of direct response experience will positively influence self-efficacy.

H7a: Higher levels of vicarious response experience will positively influence self-efficacy.

H6c: Higher levels of direct response experience will negatively influence response cost.

H7c: Higher levels of vicarious response experience will negatively influence response cost.

H8a: Higher levels of direct threat experience will positively influence threat severity.

H9a: Higher levels of vicarious threat experience will positively influence threat severity.

H8b: Higher levels of direct threat experience will positively influence threat susceptibility.

H9b: Higher levels of vicarious threat experience will positively influence threat susceptibility.

Social influence has been examined in numerous studies in the field of IS and found to be a strong direct and indirect influence in technology adoption and use (Lu, Yao, & Yu, 2005; Venkatesh et al., 2003) and a strong direct influence in secure behavioral intent (Johnston & Warkentin, 2010; Lee & Larsen, 2009). Therefore, the next set of hypotheses to be tested in the present study includes both direct and moderating effects of social influence as illustrated in Figure 3.

H10: Higher perceptions of social influence will positively influence intent to perform the recommended secure behavior.

H11a: Higher perceptions of social influence will positively moderate the relationship between self-efficacy and behavioral intent.

H11b: Higher perceptions of social influence will positively moderate the relationship between threat susceptibility and behavioral intent.

H11c: Higher perceptions of social influence will negatively moderate the relationship between response cost and behavioral intent.

H11d: Higher perceptions of social influence will positively moderate the relationship between threat severity and behavioral intent.

H11e: Higher perceptions of social influence will positively moderate the relationship between response efficacy and behavioral intent.

SETA programs are developed and implemented by organizations for the purpose of achieving employee compliance with the organization's ISP (Crossler & Belanger, 2009; D'Arcy et al., 2009; Thomson & von Solms, 1998). Persuasive messages such as fear appeals have been found to be useful in the context of encouraging secure behaviors, including behaviors of security compliance (Johnston & Warkentin, 2010). The present study proposes that SETA awareness instruction modeled after a fear appeal will result in an increase in the intention to comply with a recommended secure behavior. Also proposed is a higher intention to comply with a recommended secure behavior when

response training accompanies the fear appeal. Figure 4 illustrates the final three hypotheses developed from these propositions and the experimental component in the study.

H12: Individuals who are exposed to a fear appeal regarding an ISP threat and response will show higher intent to perform the recommended secure behavior than individuals who are not exposed to the fear appeal.

H13: Individuals who are exposed to a fear appeal and response training will show higher intent to perform the recommended secure behavior than individuals who are not exposed to the fear appeal and response training.

H14: Individuals who are exposed to a fear appeal and response training will show higher intent to perform the recommended secure behavior over that of individuals who are exposed to a fear appeal alone.

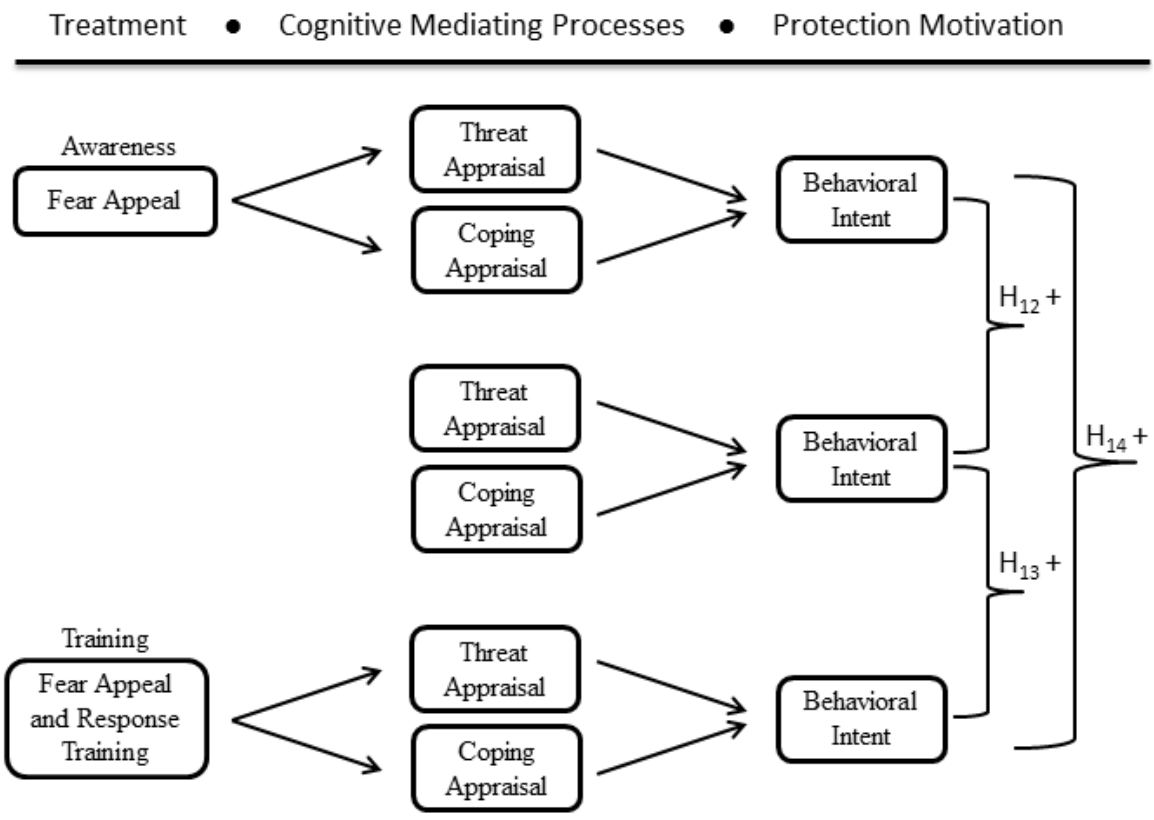

Figure 4 Model Illustrating Experimental Component and Hypotheses H12-H14

CHAPTER III

RESEARCH METHOD

Chapter III presents the methods used in this dissertation. A quantitative approach with an experimental component was selected because 1) the study builds upon prior quantitative works, 2) the relationships between latent constructs are being explored, and 3) a treatment comparison is being evaluated. This chapter begins with a presentation of the variables followed by details of the preliminary investigative procedure. Included in the preliminary investigation are details of the development of the measurement instruments and experimental treatments, validity tests, and a description of the pilot test. The chapter concludes with a discussion of the primary investigative procedure, and includes details of the experimental design, the planned analyses and hypotheses testing, the sampling frame, and procedure for the data collection and experiment.

Variables

The protection motivation theory (PMT) developed by Rogers (1975) and subsequently tested in numerous contexts in varying fields provides the theoretical foundation for this dissertation. Initially proposed as a theory to explain and consolidate fear appeal research performed in the field of Psychology, PMT was soon found to be meaningful in the field of health protection and other fields. PMT has been tested in the field of IS within the context of ISP compliance, and this study will add to that stream of research. As identified through the literature review in Chapter II, the independent

variables include threat severity, threat susceptibility, response efficacy, self-efficacy, response cost, direct response experience, vicarious response experience, direct threat experience, vicarious threat experience, and social influence, and the dependent variable is behavioral intent.

In behavioral research such as this research, individual human emotions, attitudes, perceptions, and other intangible variables are typically the phenomenon of interest to be measured. These latent variables are called constructs because, unlike objective variables such as length or weight, they cannot easily be directly and consistently observed, measured, or quantified. Since constructs cannot be directly measured, latent variable measurement scales must serve as a proxy to allow researchers to measure the phenomena they represent (DeVellis, 2003; Netemeyer, Bearden, & Sharma, 2003).

Preliminary Investigative Procedure

The preliminary procedure of this investigation began with the development of a measurement instrument and two experimental treatments. Details of the development process are discussed here along with the validity tests performed to aid in the development. The details of the experimental treatment designed for this dissertation study are presented next. This section detailing the preliminary investigative procedure concludes with a description of the pilot test.

Instrument Development

A measurement instrument was developed to collect data from the target population for the present work. The instrument includes latent variable scales to measure each construct and the treatment to be applied in the experimental components of the study. Measurement results are only as valid and reliable as the measurement

instruments (Netemeyer et al., 2003; Straub, 1989); therefore the latent variable scales utilized within the instrument, the experimental treatment component of the instrument, and the instrument itself were tested for validity and reliability.

The process used to develop the measurement instrument in the present research is illustrated in Figure 5 and includes four main steps; 1) construct definitions, 2) identification and selection of measurement items or scales, 3) if necessary, new item or scale development, and 4) instrument finalization. This process was informed by and incorporates the scale development process framework published in the seminal work by Churchill (1979) and subsequently refined, updated, and elaborated by others (Barrett, 2005; Clark & Watson, 1995; Gerbing & Anderson, 1988; Lewis, Templeton, & Byrd, 2005; MacKenzie, 2003; MacKenzie, Podsakoff, & Podsakoff, 2011; Petter, Straub, & Rai, 2007). Details of each step of the instrument development process are now presented.

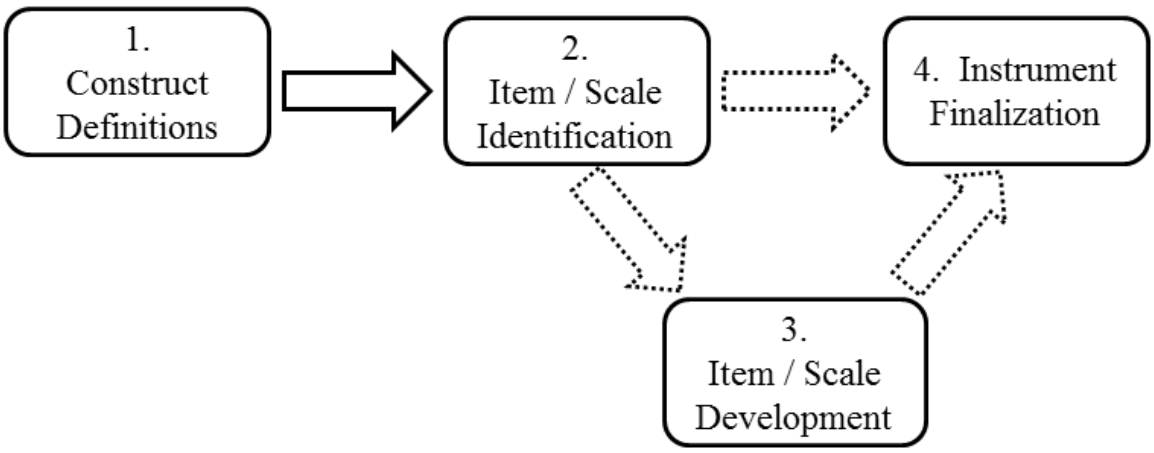

Figure 5 Instrument Development Process

Step 1 - Construct Definitions

The first step in the instrument development process is to state the theory-based definitions of the constructs as clearly and unambiguously as possible. In order to do this, a thorough literature review must be performed to determine the domain of the construct as well as to identify the boundaries of the construct, to identify the construct's use, definition, and supporting theories in prior research (Netemeyer et al., 2003). The definitions must also clearly identify the dimensionality of the construct, its level of analysis, and whether it is a formative or a reflective construct (Gerbing & Anderson, 1988; Lewis et al., 2005; Netemeyer et al., 2003; Petter et al., 2007).

The literature review that was performed and is presented in Chapter II resulted in the identification of the constructs to be included in this study. The definitions of each construct are presented in Table 4 along with their respective sources. All constructs are defined as unidimensional and reflective, and are measured at the individual level.

Table 4 Construct Definitions and Sources

Construct	Definition	Source
Threat Susceptibility	An individual's assessment of the probability of a threat occurring	Crossler (2010)
Threat Severity	An individual's perception of the significance of a threat	Johnston and Warkentin (2010)
Response Efficacy	An individual's assessment of the effectiveness of the recommended response to avert a threat	Crossler (2010)
Self-Efficacy	An individual's judgment of personal skills, knowledge, or competency about fulfilling the requirements of the response	Modified from Bulgurcu et al. (2010)
Response Cost	The overall expected unfavorable consequences for performing the response	Bulgurcu et al. (2010)
Social Influence	An individual's perception that important others believe the recommended response should be performed to avert the potential threat	Modified from Johnston and Warkentin (2010)
Direct Threat Experience	An individual's direct experience with a potential threat	Modified from Warkentin et al. (2011)
Direct Response Experience	An individual's direct experience with a response to a threat	Modified Warkentin et al. (2011)
Vicarious Threat Experience	An individual's indirect experience with a potential threat through observation	Warkentin et al. (2011)
Vicarious Response Experience	An individual's indirect experience with a response to a threat through observation	Warkentin et al. (2011)
Behavioral Intent	An individual's intention to perform the recommended response to avert the potential threat	Johnston and Warkentin (2010)

Step 2 - Item and Scale Identification

The second step in the development of a measurement instrument is to identify a scale to measure each construct. Developing new scales to measure a construct is a time consuming and sometimes arduous process. Furthermore, after new latent variable measurement scales are developed and validated, the performance of confirmatory tests within other contexts and populations is necessary to strengthen the findings of validity and reliability and to add to the generalizability of the scales (Netemeyer et al., 2003; Straub, 1989). Therefore, rather than developing new scales, the literature review can facilitate the identification of previously validated scales that may be adapted for use within the current context. This is recommended not only as a more efficient research

method, but also because it results in a continuing contribution to and strengthening of the research community.

The present research sought out previously validated latent variable scales from published works that were appropriate for adaptation to the context of the current study. No existing scales were found to fit the four experience construct definitions, but scales were identified for all other constructs. The measurement scales for threat severity (TSV), social influence (SOC), and behavioral intent (BEH) were adapted from Johnston and Warkentin (2010) who stated that social influence and behavioral intent had been adapted from Venkatesh et al. (2003) and threat severity had been adapted from Witte, Cameron, McKeon, and Berkowitz (1996). The measurement scales for threat susceptibility (TSU) and response efficacy (REF) were adapted from Crossler (2010), who stated they were originally adapted from Witte et al. (1996). The scales for self-efficacy (SEF) and response cost (RSC) were adapted from scales developed by Bulgurcu et al. (2010).

When confirmatory testing of existing scales is performed, minor adaptation of measurement items is often necessary and is typically achieved through a modification of the wording to fit the study context. Because the social influence scale is defined by Johnston and Warkentin (2010) as formative but the construct is defined in this study as reflective, the one scale item that most closely represents the domain of social influence within the context of this study was selected and subsequently adapted through rewording to fit the current context. Two additional measurement items were then developed to create a three-item reflective scale. Care was taken to follow the primary decision rules to ensure the scale was reflective (Petter et al., 2007). Specifically, 1) the items reflect the construct, they do not define it, 2) the scale is unidimensional; 3) the measures have

the same antecedents and consequences; and 4) the items are expected to co-vary and statistical tests were run to confirm. The measurement items in the remaining existing scales were adapted for the present study through slight rewording to fit the current context. The constructs with adapted measurement items and the literary sources for each scale are shown in Table 5.

Table 5 Adapted Reflective Measurement Scales

Construct & Source		Measurement Items
Likert scale where 1 = Strongly Disagree and 5 = Strongly Agree		
Threat Susceptibility (Crossler, 2010)	TSU1	I am at risk for data loss.
	TSU2	It is likely that I may lose data.
	TSU3	It is possible that I may lose data.
Threat Severity (Johnston & Warkentin, 2010)	TSV1	If I lost data, it would be a severe problem.
	TSV2	If I lost data, it would be a serious problem.
	TSV3	If I lost data, it would be a significant problem.
Response Efficacy (Crossler, 2010)	REF1	Data backups work for protection against data loss.
	REF2	Data backups are effective to prevent data loss.
	REF3	Performing data backups will guard against data loss.
Self-efficacy (Bulgurcu et al., 2010)	SEF1	I am confident I have the skills needed to back up data.
	SEF2	I believe I have the knowledge necessary to back up data.
	SEF3	I know I could successfully back up data.
Response Cost (Bulgurcu et al., 2010)	RSC1	Backing up data is time consuming.
	RSC2	Backing up data is a burden.
	RSC3	Backing up data is inconvenient.
Social Influence (Johnston & Warkentin, 2010)	SOC1	People who influence my behavior think that I should perform data backups.
	SOC2	People who are important to me think that I should perform data backups.
	SOC3	In general, others think that I should perform data backups.
Behavioral Intent (Johnston & Warkentin, 2010)	BEH1	I intend to backup data at least once in the next month.
	BEH2	I predict I will backup data at least once in the next month.
	BEH3	I plan to backup data at least once in the next month.

Because no existing scales were identified that fit the definitions of the four experience constructs, new measurement scales were developed. The next section presents details of the development process.

Step 3 - Item and Scale Development

When a literature review fails to identify previously validated measurement scales appropriate for adaptation to the context of a study, the third step of the instrument development process is necessary. New measurement scales are developed in this step. Items that either reflect or form the construct, depending upon the construct definition, are created (Churchill, 1979; Lewis et al., 2005; MacKenzie et al., 2011). The goal of this step is to develop a scale by including items that together will fully reflect the domain of the construct. Meeting that goal relies on the literature review, the construct definition, and the theoretical foundation of the study. A latent variable scale for vicarious experience (Warkentin et al., 2011) was identified during the literature review which, although not specifically appropriate for use or modification in this dissertation study, did serve to inform the development of the definitions and new measurement scales for the four experience constructs direct threat experience (DTE), direct response experience (DRE), vicarious threat experience (VTE), and vicarious response experience (VRE).

The construct of experience, its definition, its treatment, and its measurement has been examined in IS literature and found lacking in consistency and clarity (Aguirre-Urreta & Marakas, 2008). The experience construct is typically poorly defined, and an actual definition is rarely provided. Experience is frequently a measurement of quantity and thus measured through a single indicator such as years of experience (Constant,

Sproull, & Kiesler, 1996) or the number of times an occurrence has been experienced (Sitren & Applegate, 2007). It is also often seen as a multi-dimensional or formative construct, for example to measure a consumer's service experience (Kim, Cha, Knutson, & Beck, 2011) or an individual's experience with cybercrime (Boss, Kirsch, Angermeier, & Boss, 2009). Experience is a broad construct and its meaning may be subjective depending upon the research context. In this dissertation, the experience constructs are defined (see Table 4) as unidimensional reflective constructs and the measures will attempt to capture the individual or observed experience with a specific information security threat and with a specific information security response.

Following the generally accepted methods of reflective scale development (Churchill, 1979; Netemeyer et al., 2003), at least three measurement items for each construct were generated based on the construct definitions and guided by the underlying theory of PMT. Additionally, in order to reduce potential common method bias (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003), care was taken to ensure that each of the items was clearly worded, was not ambiguous, and was focused upon a single issue for which a single answer would suffice. The experience construct definitions along with the new measurement scales are shown in Table 6.

Table 6 New Reflective Experience Measurement Scales

Construct	Measurement Items Likert scale where 1 = Strongly Disagree and 5 = Strongly Agree
Direct Threat Experience: An individual's direct experience with a potential threat	
DTE1	I have experienced losing data.
DTE2	Data loss has happened to me.
DTE3	Data loss is something I have experience with.
Direct Response Experience: An individual's direct experience with a response to a threat	
DRE1	I have experience performing data backups.
DRE2	I have performed data backups.
DRE3	Backing up data is something I have experience with.
Vicarious Threat Experience: An individual's indirect experience with a potential threat through observation	
VTE1	I know someone who has experienced losing data.
VTE2	Data loss has happened to someone I know.
VTE3	Data loss is something others I know have experience with.
Vicarious Response Experience: An individual's indirect experience with a response to a threat through observation	
VRE1	I know someone who has experience performing data backups.
VRE2	I know others who have performed data backups.
VRE3	Backing up data is something others I know have experience with.

Note: Experience definitions and scales informed by (Warkentin et al., 2011)

Step 4 - Instrument Finalization

Finalization of the instrument includes testing the face and content validity of the scale items of each construct, and of the instrument itself (Netemeyer et al., 2003). Validity testing is followed by a pilot test conducted with a small number of respondents drawn from the population representative of that of the primary study. An exploratory factor analysis, and reliability and validity testing of the pilot data collected should then be conducted.

The validity of an instrument is determined through assessment of its face validity and its content validity (Netemeyer et al., 2003). Face validity refers to the wording of the items and the overall look of the instrument. All components of the instrument should be tested for face validity, including components such as the instructions and such

as the format of the responses. The items and instructions should be written such that they are clear and easily understood by the intended respondent population. The instrument should be attractive and be constructed with consistency and proper item flow. Content validity refers to the need for the items to encompass the full domain of the construct while maintaining clarity and consistency.

Experimental Treatments

The specific context explored in this research work is the use of a fear appeal to affect individual information security policy (ISP) compliance behavior. Two experimental treatments were utilized and compared in this dissertation. As discussed in Chapter I, three levels of instruction are typically included in SETA programs conducted by organizations to encourage employee compliance with ISP. The levels are awareness, training, and education. The awareness level informs individuals of the "what" regarding an information security threat and response. The training level informs individuals of the "how" regarding an information security threat and response. The education level informs individuals of the "why" regarding an information security threat and response. As stated earlier in this dissertation and as indicated by research question 3, the awareness and training levels are the treatments that are being tested and compared in this dissertation. The education instructional level is too high a level of instruction to be practical for the majority of employees in a typical organization; therefore, it is not being addressed.

Treatment 1 emulated the awareness level of instruction that was modeled after a fear appeal persuasive message. It consisted of an informative message which included the four components of a fear appeal (the threat is severe, is likely to occur, the response

works, and is easy to use) and contained the definitions of a threat and a response (awareness). Treatment 2 was the same as Treatment 1 with an additional element consisting of instructions regarding use of the recommended response, thereby emulating the training level of a SETA program. In the context of information security, numerous different threats are possible and frequently more than a single response is available to guard against each threat. The selection of an information security issue upon which to focus in this study was necessary. The information security threat selected was electronic data loss and the corresponding response to the threat was data backups. This threat and response pair is appropriate for this study because it represents a persistent information security problem and one that is typically addressed in SETA programs.

Validity Testing

Assessment of face and content validities of the measurement instrument and of the treatments was achieved through use of a panel of experts knowledgeable in the area of the study and in latent variable measurement in general. The instrument prepared for expert panel review needed to include all of the measures and treatment components possible. Because the pretest and the posttest was identical and because Treatment 2 included Treatment 1, the instrument prepared consisted of the introduction, instructions, Treatment 2, the posttest, and the demographic items. Two expert panel review sessions were conducted. The first group reviewed the instrument on paper in a face-to-face setting. The second group reviewed the instrument online, individually on their own using the browser of their own preference.

The panel members of the face-to-face panel suggested that the self-efficacy and response cost construct measurement scales were too closely related and alternate scales

were suggested. Wording change suggestions were made for the new experience scales to better reflect the constructs and increase the readability. Changes to the formatting and overall wording of the experimental treatments were suggested. The domains of the response cost and self-efficacy constructs were reassessed and alternate existing scales were selected for use in the study. Other comments and recommendations made by the panel were considered and appropriate changes were made to the instrument.

The second expert panel session took place a few weeks later. The review panel members were invited via email to view the revised instrument and provide feedback. The email sent to panel members included a document attached that provided a link to the survey and also a brief review of the study. After about one week, the comments were collected from the online survey host, reviewed and summarized. A few minor wording changes to the treatments were suggested, and the recommended changes were accepted and implemented. The other comments made were related to presentation and formatting of the instrument in the online environment. Corrections and adjustments were made and the online instrument was finalized. The same version of the final measurement instrument with experimental treatments is shown in Appendix B.

Pilot Test and Data Analysis

After receiving feedback from the expert panel, the measures were refined and a pilot test was performed. The pilot instrument consisted of the introduction, instructions, the pretest, Treatment 2, the posttest, and the demographic items. The pilot test was conducted in a web-based environment using the online survey host Qualtrics. The survey was conducted with a small sample from the intended respondent population. An arrangement was made with three instructors of classes in the MSU College of Business

during the mini session known as Maymester in the summer of 2012. An offer of extra credit in exchange for participation in the pilot study was made to the enrolled students. After removing incomplete data cases, a total of 65 students were found to have completed the pilot study.

The data collected was analyzed for item discriminant and convergent validity, and internal reliability of scales. No issues with the items were identified and the instrument was deemed ready for the primary data collection.

To test for reliability and validity during instrument development and the preliminary data collection phase, the statistical software package IBM SPSS version 20 was utilized. To test for convergent validity and discriminant validity, data was analyzed through exploratory factor analysis (EFA). Inspection of the item loadings was performed to verify the items of each construct loaded together representing convergent validity of the items, and that no strong cross-loadings exist between items of different scales which would represent discriminant validity.

Primary Investigative Procedure

The primary investigative procedure of this dissertation study includes the collection of data by means of a web-based survey instrument. Because a treatment was being tested, an experimental treatment design was also imposed. Analysis of the data was accomplished using well-established statistical methods aided by current statistical software packages commonly used by researchers in similar research endeavors. The details of this procedure are discussed now.

Experimental Design

After the instrument was developed and validated through the use of an expert panel and pilot study data analysis, the primary data collection was performed. The data collection method uses the Solomon Four-Group Design and includes the use of a survey instrument pretest, an experimental component, and a survey instrument posttest within a randomized control group design. The pretest included the same measurement items as the posttest.

Solomon Four-Group Design

When developing a data collection method, the validity of the data, ensuring what was measured was in fact what was intended to be measured, is necessary for the results to be meaningful. Both internal and external validity threats can be controlled through careful research design. In the case of this study, an experimental treatment was used and therefore a control group was required for comparison and verification of the effect of the treatment.

There are several factors that may affect the internal or external validity of an experimental design (Campbell & Stanley, 1963). Verification that an experiment possesses internal validity is a necessity as evidence of this validity is equivalent to evidence of treatment effectiveness. External validity concerns the question of generalizability of the experiment with regards to populations and variables. Internal validity may be negatively affected by several factors such as the effects of maturation, instrumentation, or selection bias. Several factors may negatively affect external validity as well, such as the existence of interaction effects between selection biases and the experimental variable, by reactive effects of experimental arrangements, by multiple-treatment interference, or by an interaction effect by the pretest. Most of the basic

experimental methods adequately protect against the internal validity threats, but because of its ability to also assess the existence of pretest interaction, the Solomon Four-Group Design is typically considered the best choice (Braver & Braver, 1988; Levy & Ellis, 2011; Sawilowsky, Kelley, Blair, & Markman, 1994).

The experimental method of Solomon Four-Group Design (S4G) is an ideal method as it controls internal validity threats and enables detection of effects of the pretest on the treatment which also provides evidence of external validity in the form of generalizability to other populations (Braver & Braver, 1988; Campbell & Stanley, 1963). The S4G entails randomly assigning respondents into one of four possible groups which will receive a combination of a pretest, treatment, and posttest, as illustrated in Figure 6. In this dissertation study, the measures in the pretest are the same as those in the posttest. The first group, Group A, is given the pretest, followed by the treatment, and then the posttest. Group B is given only the pretest and posttest, Group C is given the treatment followed by the posttest, and Group D receives only the posttest. Groups A and C are the experimental groups and Groups B and D are the control groups which are used as the baseline measures to compared to the experimental groups to validate the effect of the treatment (Levy & Ellis, 2011).

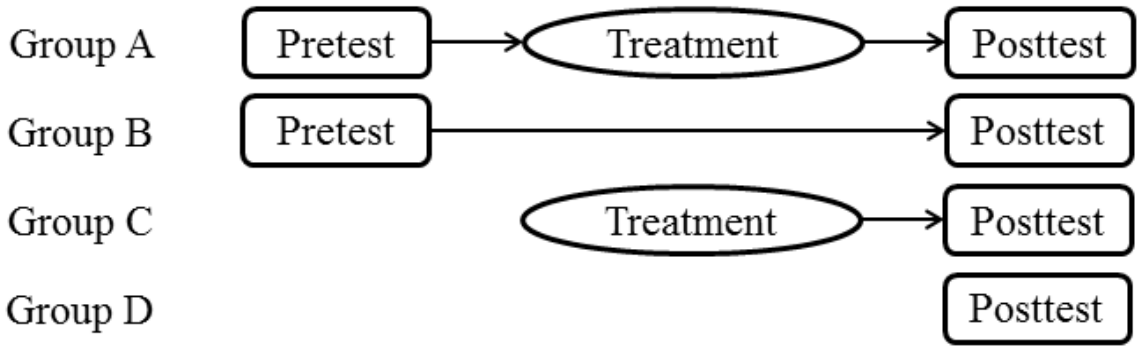

Figure 6 Solomon Four-Group Design

Note: Adapted from Vogt (2005)

While few disagree with the assessment that the S4G is a highly rigorous method choice, the design is nonetheless rarely selected for use by researchers. One reason likely to be a main contributor to the paucity of the design's use is the high number of respondents required. Each of the four groups in the design must include a minimum of 30 respondents in order to meet the statistical requirements to test group differences (Pallant, 2005; Yount, 2006), equating to a minimum of an additional 60 respondents required due to the inclusion of the control groups. Additionally, disagreement exists regarding the specific statistical techniques necessary to properly and fully assess this experimental design (Braver & Braver, 1988; McGahee & Tingen, 2009; Sawilowsky et al., 1994; Shuttleworth, 2009), but the general consensus is to conduct a series of t-tests and analysis of variance (ANOVA) of the groups' pretest and posttest DV means as an acceptable validity analyses technique.

The analysis of data collected using the S4G includes performance of several group comparisons. The four groups are shown in Figure 6 and consist of two experimental groups, Groups A and C, and two control groups, Groups B and D. To verify no influence from the pretest, the posttest results of Groups A and B are compared

to the posttest results of Groups C and D. To attain evidence of external validity, Group B pretest and Group D posttest are compared. Groups A and C posttests are compared to verify the existence of a treatment effect. A comparison of the posttests of Group B and Group D is performed to verify there is no significant difference between them which is evidence that the pretest had no influence (Shuttleworth, 2009).

Modified Solomon Four-Group Design

Because two treatments were included in the experiment, the Solomon Four-Group Design was modified to include additional groups to accommodate the second treatment. The modified Solomon Four-Group Design (MS4G) as shown in Figure 7 includes two primary experimental groups, Groups A_1 and A_2, two secondary experimental groups, Groups C_1, C_2, and two control groups, Groups B and D.

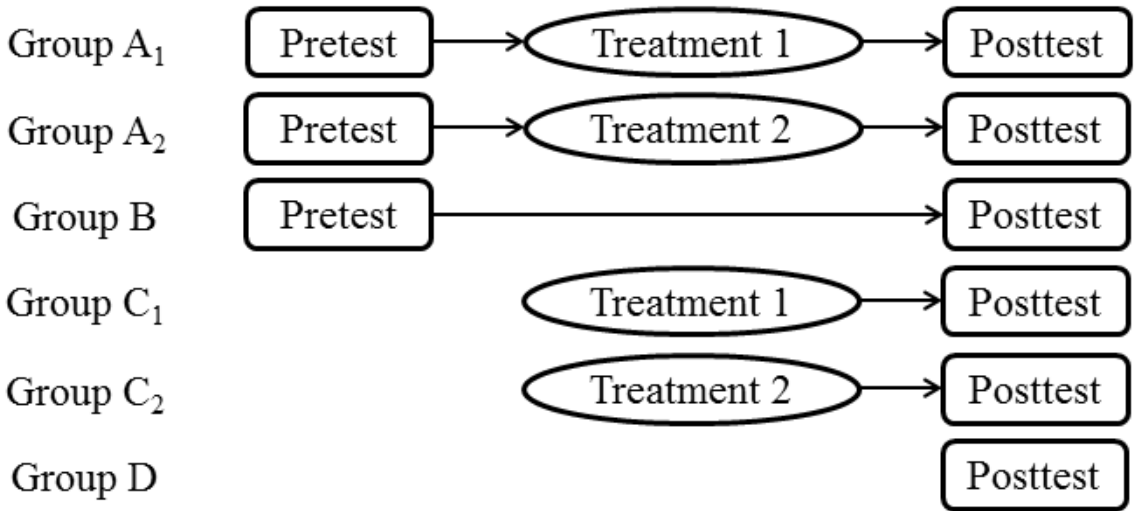

Figure 7 Modified Solomon Four-Group Design

Note: Adapted from (Vogt, 2005)

Table 7 describes the two treatments with Treatment 1 consisting of a fear appeal which contains the four necessary fear appeal components, and includes the definitions of the threat and response. Treatment 2 consists of the same fear appeal with definitions plus training regarding the recommended response to the threat.

Table 7 Experimental Treatments

Treatment	Purpose	Description
Treatment 1	Awareness	Fear Appeal with Threat & Response Definitions
Treatment 2	Training	Treatment 1 + Response Instruction

The primary experimental Groups A_1 and A_2 were provided with the pretest, exposure to a treatment, and the posttest. Group A_1 received Treatment 1, and Group A_2 received Treatment 2. Group B received the pretest and posttest only. Group C_1 received Treatment 1 followed by the posttest, and Group C_2 received Treatment 2 followed by the posttest. Finally, Group D received the posttest only.

Data Analysis and Hypotheses Testing

The data collected in this study through the MS4G experimental method was used to conduct 1) analyses of the experimental component, 2) exploratory analyses of the latent variable measures, and 3) confirmatory analyses of the measurement model and the structural model.

Experimental Component Analyses

The experimental component data analyses were performed to verify external and internal validity of the experimental method, and to test Hypotheses 12-14 (listed in Chapter II). External validity was tested through two 2x2 ANOVA and one 2x3

ANOVA tests on the posttest group score means to verify that there was no influence from the pretest. To test internal validity, a series of t-tests were performed. The tests included comparisons of the pretest and posttests of the A Groups and the C Groups to verify the existence of a treatment effect. A comparison of the posttests of Groups B and D was performed to verify there was no significant difference between them and to provide evidence that the pretest had no influence.

Exploratory Analyses of Measures

The primary data collected was analyzed in the same manner as the preliminary data as described previously, again using the statistical software package IBM SPSS version 20. An exploratory factor analysis (EFA) was conducted on the primary data collected. Principal Components Analysis is the preferred factor analysis technique for EFA because it produces a summarization of the data by extracting a set of components, or factors, that describe the relationships among the variables (Tabachnick & Fidell, 2007). The factors were rotated after extraction to enhance their interpretation. The rotation selected was Varimax because it is the most commonly used orthogonal rotation and because it is most likely to reveal the simple structure of the factors (Hair, Black, Babin, & Anderson, 2010; Netemeyer et al., 2003; Tabachnick & Fidell, 2007). Convergent validity and discriminant validity tests were performed through the inspection of the factor loadings. Internal reliability was assessed using an examination of the Coefficient Alpha values which is the most commonly preferred method of assessment (Churchill & Peter, 1984; Peter, 1979; Peterson, 1994).

Confirmatory Measurement Model and Structural Model Analyses

After completing the EFA analyses, the measurement model and the structural model were assessed. Structural Equation Modeling (SEM) is a group of statistical techniques that are particularly useful in behavioral research because they provide highly rigorous confirmatory factor analyses, path model analyses, and allow for simultaneous analyses of measurement and prediction (Kelloway, 1998; Kline, 2011). The approach used was the recommended two-step approach (Anderson & Gerbing, 1988) where a confirmatory analysis is performed on the measurement model first to establish evidence of construct validity and followed by a confirmatory analysis on the structural model to establish evidence of nomological validity. The statistical software package IBM SPSS Amos version 20 was used to conduct the confirmatory factor analysis (CFA) on the measurement model. The results of the measurement model analysis were examined for evidence of reliability and validity at the item level and at the construct level. After the measures were found to be valid, an analysis on the structural model was performed. Hypotheses 1-10 (listed in Chapter II and illustrated in Figure 3) were tested through the examination of the model fit statistics and path coefficients. Tests were performed to determine what, if any, moderating effects by the Social Influence construct were present, thereby testing Hypotheses 11a-11e. The results of all the data analyses are presented in Chapter IV.

Sampling Frame

The present study used an online experiment and survey instrument to collect data from a population which included the faculty, staff, and students at Mississippi State University (MSU). A campus-wide announcement email was disseminated, inviting the members of the MSU community to participate in the study. The snowball method was

also used, and was operationalized through the inclusion of a request to forward the email to friends, family, and coworkers. The MSU population is diverse ("Diversity Statistics - Campus Wide," 2011) and all members of the MSU student and employee population are required to comply with information security policies (ISP). Furthermore, it is expected that faculty, staff, and students have data stored on their computers that is important or that they do not wish to lose and is therefore a representative sampling of the population of interest for the study. However, to determine whether this was indeed the case, the measurement instrument included the question "Do you regularly use a computer that also stores personal, sensitive, or valuable information that you want protected?"

CHAPTER IV

ANALYSES AND RESULTS

The analyses and results of this study are presented in this chapter. First a discussion of the analyses and results of the pilot study is presented, followed by the primary study analyses and results. The software tools used for statistical analyses were IBM SPSS Statistics version 20 and IBM SPSS Amos version 20. The primary purpose of the pilot study was to test the performance of the latent variable scales; therefore, the analyses included an exploratory factor analysis (EFA) to test for convergent and discriminant validity, and internal reliability tests for each measurement scale. The primary study analyses repeated the EFA, and included a confirmatory factor analysis (CFA) to test for convergent and discriminant validity, and also included internal reliability tests. Additionally, the analyses specific to use of the MS4G were conducted which included a series of t-tests and ANOVA tests. Finally, the hypotheses were tested through use of structured equation modeling techniques. Each of these tests and the results obtained are discussed.

Pilot study analyses

The pilot sample was drawn from undergraduate students attending classes in the College of Business at Mississippi State University. Table 8 contains the demographic details of the pilot study sample. The total number of respondents in the pilot study was 64. The time to complete the survey was estimated to be 15 minutes, and students took an average of just over 14 minutes which confirmed that the completion time estimate

was accurate. Beyond the content and face validity evaluations of the scales, of the treatments, and of the instrument as a whole as described in Chapter III, an EFA analysis was performed to test the convergent and discriminant validity of the latent variable scale items, and a test of internal reliability was also performed for each measurement scale.

Table 8 Pilot Study Respondent Sample Characteristics

Demographic		**Count (N)**	**Percentage (%)**
Gender	Male	30	46.9
	Female	34	53.1
Age	18-19	5	7.81
	20-29	56	87.5
	30-39	1	1.56
	40-49	1	1.56
	Missing Data	1	1.56
Position	Student	62	96.9
	Staff	1	1.6
	Faculty	0	0.0
	Other	1	1.6
Education	High School	13	20.3
	Some College	35	54.7
	Associate's	12	18.8
	Bachelor's	4	6.3
	Master's	0	0.0
	Doctoral	0	0.0
Years of Computing Experience	Fewer than 3	4	6.3
	3-9	19	29.7
	10-24	41	64.1
	25 or more	0	0.0
Years of Work Experience	Fewer than 3	27	42.2
	3-9	32	50.0
	10-24	4	6.3
	25 or more	1	1.6

Exploratory Factor Analysis

All pilot study participants received the pretest, Treatment 2, and the posttest. The pretest and the posttest were identical, and separate analyses were initially conducted on the two data sets. Similar results were obtained for both sets so the pretest data was used to conduct the full pilot study analyses. This decision was made to exclude any potential effects by the treatment or multiple instances of exposure to the scale items on the responses by the participants.

Because the pilot study goal was to gauge whether the measurement scales would perform as expected and to make changes prior to conducting the primary study, the EFA analysis focused on a basic assessment of the scale items. The EFA was conducted using the statistical technique of Principal Components Analysis with Varimax rotation. (Hair et al., 2010; Netemeyer et al., 2003; Tabachnick & Fidell, 2007).

The EFA of this pilot test revealed eight rather than eleven factors based on the Eigen-value-greater-than-one rule; however, because *a priori* theory indicated the presence of eleven factors, the analysis was repeated with a forced extraction of eleven factors. The results of the eleven-factor EFA showed communalities greater than .30. The rotated component matrix revealed all items loading at no less than 0.40 on at least one factor. This evidence verified that all items met the minimal level of interpretability and indicated they should all be retained (Hair et al., 2010; Netemeyer et al., 2003).

Examination of the rotated components matrix revealed many of the item factors loaded on separate factors at levels exceeding the preferred threshold of .70 (Hair et al., 2010) with no cross loadings greater than 0.40 which indicated good convergent and discriminant validity for those items. However, a few item factor loading values were lower than preferred and there was evidence of cross-loading among the variables. The

Scree plot suggested a ten-factor solution was plausible; therefore the EFA was repeated with only ten factors and the solution was compared to the eleven-factor solution. The ten-factor solution, presented in Table 9, revealed fewer loadings at values lower than .70. Cross-loadings were again evident, but found only among Self-efficacy, the four new experience constructs, and Behavioral Intent. The results of these EFA suggested acceptable convergent and discriminant validity for this pilot study.

Table 9 Pilot Study EFA Analysis Ten-factor Rotated Component Matrix[a]

	Component									
	1	2	3	4	5	6	7	8	9	10
TSU1			.725							
TSU2			.867							
TSU3			.702							
TSV1		.866								
TSV2		.904								
TSV3		.794								
REF1								.841		
REF2								.819		
REF3								.654		
SEF1	.882									
SEF2	.876									
SEF3	.835									
RSC1						.658				
RSC2						.926				
RSC3						.834				
SOC1				.848						
SOC2				.822						
SOC3				.854						
DTE1					.863					
DTE2					.846					
DTE3	.408				.738					
DRE1	.833									
DRE2	.835									
DRE3	.747									
VTE1			.524							.473
VTE2			.605							.413
VTE3							.764			
VRE1										.622
VRE2							.733			
VRE3							.739			
BEH1	.542			.407					.512	
BEH2	.582								.413	
BEH3	.601									

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 10 iterations.

The internal consistency estimates were calculated for each construct as well, and the coefficient alpha scores for each construct are shown in Table 10. The alpha values were greater than .70, indicating good scale reliability for all measurement scales (Clark & Watson, 1995; Hair et al., 2010; Netemeyer et al., 2003). Overall, the results of the pilot test indicate that all measurement items should be retained and no changes were necessary before proceeding to conduct the primary data collection.

Table 10 Pilot Study Construct Reliability Analysis Results

Construct	Construct Name	Alpha
TSU	Threat Susceptibility	0.834
TSV	Threat Severity	0.894
REF	Response Efficacy	0.803
SEF	Self-efficacy	0.907
RSC	Response Cost	0.837
SOC	Social Influence	0.867
DTE	Direct Threat Experience	0.914
DRE	Direct Response Experience	0.896
VTE	Vicarious Threat Experience	0.796
VRE	Vicarious Response Experience	0.786
BEH	Behavioral Intent	0.940

Primary Study Analyses

This section presents the results of the analyses of the primary data collection phase of the study. Three main sets of analyses were conducted. The first set consisted of t-tests and ANOVA tests to gather validity evidence for the experimental component of the study and to test Hypotheses 12-14. The second set consisted of an exploratory factor analysis of the measures. The third set consisted of a confirmatory factor analysis of the measurement and structural models to gather evidence of validity, reliability, model fit, and to test Hypotheses 1a-10. Additionally, the moderating effects of the Social Influence construct on the predictive paths indicated in Hypotheses 11a-11e were

tested. The remaining portion of this section includes the results of the three analyses sets, beginning with the characteristics of the sample analyzed.

Sample Characteristics

An invitation to participate in this dissertation study was emailed to the entire Mississippi State University (MSU) campus consisting of approximately 25,000 students, faculty, and staff ("Mississippi State University Pocket FactBook," Fall 2011). The email invitation included a request to forward the email to others outside the MSU community. This sampling technique known as the snowball method expanded the number of invitees beyond the MSU community. To further expand the potential respondent pool, a participation invitation was posted on two individual's personal pages of the social networking website Facebook. Additionally, an email invitation was sent to the members of the Association for Information Systems on two separate occasions through their membership listserv.

An email survey such as the one conducted in this dissertation where an entire group's or an organizational membership is invited to participate yet the respondents are allowed to self-select their participation is known as an opt-in survey (AAPOR, 2012; de Leeuw, Hox, & Dillman, 2008). Because there was not a random sampling performed from the intended population, a reporting of a calculated response rate that implies such would be misleading and therefore is not reported in this dissertation.

A total of 633 individuals accessed the online instrument. Prior to conducting statistical analyses, the data was cleaned and cases with missing pretest or posttest data were removed. A total of 311 responses were found to be complete. The characteristics of the respondents, shown in Table 11, included about half male and half female and

representing ages from 18 to over 80, with the majority in the age range of 20 to 39. The number of students, faculty, and staff were nearly equally represented at about 30% each. As expected, the respondents in the sample were well educated with the majority reporting either a bachelor's, a master's, or a doctoral degree had been earned. Sixty-four percent of the respondents reported having at least 10 years of work experience and 88% reported at least 10 years of computing experience.

Table 11 Primary Study Respondent Sample Characteristics

Demographic		Count (N)	Percentage (%)
Gender	Male	142	45.7
	Female	158	50.8
	Missing data	11	3.5
Age	18-19	7	2.3
	20-29	81	26
	30-39	81	26
	40-49	60	19.3
	50-59	51	16.4
	60-69	15	4.8
	70-79	1	0.3
	> 80	1	0.3
	Missing data	14	4.5
Position	Student	95	30.5
	Staff	91	29.3
	Faculty	96	30.9
	Other	23	7.4
	Missing data	6	1.9
Education	High School	9	2.9
	Some College	38	12.2
	Associate's	15	4.8
	Bachelor's	72	23.2
	Master's	89	28.6
	Doctoral	83	26.7
	Missing Data	5	1.6
Years of Computing Experience	Fewer than 3	4	1.3
	3-9	29	9.3
	10-24	187	60.1
	25 or more	86	27.7
	Missing Data	5	1.6
Years of Work Experience	Fewer than 3	32	10.3
	3-9	76	24.4
	10-24	118	37.9
	25 or more	80	25.7
	Missing data	5	1.6

Validity of the Experimental Method

A series of t-tests and ANOVA tests were conducted comparing the experimental and control groups to seek out and confirm the existence of evidence of internal and external validity of the experiment. To meet the statistical requirements of the group comparison tests, a total of 30 cases were randomly selected from each of the groups. These equal-size groups were used to conduct the comparison tests.

External Validity

Because two treatments were tested, the external validity of the experiment was tested by conducting two 2x2 ANOVA and one 2x3 ANOVA tests on the posttest score means of the groups to test for an interaction effect from the pretest. The design of the ANOVA tests required the creation of dummy variables. One dummy variable was created to signify whether the pretest was received with 0=no and 1=yes. Another dummy variable was created to signify which treatment was received, with 0=No Treatment, 1=Treatment 1, and 2=Treatment 2.

A primary assumption of the ANOVA test is that the variance of the DV is equal across groups; therefore, the Levene's Test for Equality of Variances was conducted. As shown in Table 12, the results of the Levene's tests in all three of the ANOVA tests were not statistically significant, indicating the group variances were homogeneous and signifying that the assumption for each ANOVA was met and the results could be examined.

Table 12 Levene's Test of Equality of Error Variances[a]

Groups	F	Df1	Df2	Sig.
A_1, B, C_1, D	2.046	3	116	.111
A_2, B, C_2, D	1.824	3	116	.147
A_1, A_2, B, C_1, C_2, D	1.454	5	174	.207

a. Design: Intercept + Pre + Treatment + Pre * Treatment

To test Treatment 1, the first 2x2 ANOVA was a standard S4G group comparison run using Groups A_1, B, C_1, and D. To test Treatment 2, another standard S4G 2x2 ANOVA was run using A_2, B, C_2, and D. The 3x2 ANOVA was a MS4G group comparison that tested all six of the groups. The purpose of these ANOVA tests was to verify external validity of the experimental method and is determined through an examination of the interaction between the pretest and the treatment. The results of the ANOVA tests revealed no statistically significant interaction effect between the pretest and the treatment (Pre*Treatment), as detailed in Table 13. Because the pretest did not influence the treatment, there is evidence of external validity of the experimental method.

Table 13 Tests of Between-Subjects Effects

	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
2x2 Groups: A_1, B, C_1, D						
Corrected Model	5.781[a]	3	1.927	1.824	.147	.045
Intercept	1715.112	1	1715.112	1623.419	.000	.933
Pre	5.490	1	5.490	5.196	.024	.043
Treatment	.268	1	.268	.253	.616	.002
Pre * Treatment	.023	1	.023	.022	.883	.000
Error	122.552	116	1.056			
Total	1843.444	120				
Corrected Total	128.332	119				
2x2 Groups: A_2, B, C_2, D						
Corrected Model	4.336[b]	3	1.445	1.228	.303	.031
Intercept	1640.334	1	1640.334	1393.454	.000	.923
Pre	4.156	1	4.156	3.531	.063	.030
Treatment	.156	1	.156	.133	.716	.001
Pre * Treatment	.023	1	.023	.020	.889	.000
Error	136.552	116	1.177			
Total	1781.222	120				
Corrected Total	140.888	119				
2x3 Groups: A_1, A_2, B, C_1, C_2, D						
Corrected Model	8.131[c]	5	1.626	1.484	.197	.041
Intercept	2518.765	1	2518.765	2298.683	.000	.930
Pre	7.200	1	7.200	6.571	.011	.036
Treatment	.838	2	.419	.383	.683	.004
Pre * Treatment	.093	2	.046	.042	.959	.000
Error	190.659	174	1.096			
Total	2717.556	180				
Corrected Total	198.790	179				

a. R Squared = .045 (Adjusted R Squared = .020)
b. R Squared = .031 (Adjusted R Squared = .006)
c. R Squared = .041 (Adjusted R Squared = .013)

Internal Validity

To test the internal validity of the experiment, the groups were compared through a series of t-tests for the purpose of verifying treatment effectiveness and to test for

differences in the treatments. The tests performed are described in Table 14 along with the literature sources.

Table 14 Internal Validity T-Test Descriptions

Groups Compared		Purpose of Test	Literature Source
Paired Samples			
A_1 Pretest	A_1 Posttest	Treatment 1 effectiveness	(Kirk, 2009; McGahee & Tingen, 2009)
A_2 Pretest	A_2 Posttest	Treatment 2 effectiveness	
Independent Samples			
A_1 Posttest	A_2 Posttest	Difference in Treatments	(McGahee & Tingen, 2009; Shuttleworth, 2009)
A_1 Posttest	B Posttest	Treatment 1 effect	
A_2 Posttest	B Posttest	Treatment 2 effect	

A paired samples t-tests was performed on Group A_1 to test the effectiveness of Treatment 1 and on Group A_2 to test the effectiveness of Treatment 2. To determine these effects, the DV means of the pretest scores were compared to the DV means of the posttest scores in the two experimental groups. The results of these first two t-tests are shown in Table 15. No significant difference was found for either group indicating neither Treatment 1 nor Treatment 2 contributed toward changing the respondents' behavioral intent.

Table 15 Treatment Effectiveness - Paired Samples T-Tests Groups A_1 and A_2

	Paired Differences							
				95% CI of the Difference				
Means Compared	**Mean**	**Std. Dev.**	**Std. Error Mean**	**Lower**	**Upper**	**t**	**df**	**Sig. (2-tailed)**
A_1 Pretest = 4.0778 A_1 Posttest = 4.0556	.02222	.68332	.12476	-.23293	.27738	.178	29	.860
A_2 Pretest = 3.8889 A_2 Posttest = 3.8333	.05556	.29143	.05321	-.05327	.16438	1.044	29	.305

Three independent samples t-tests were then performed. The first t-test was performed to compare the DV means of the posttest scores of Groups A_1 and A_2 to determine whether there was any difference between the two treatments effectiveness. Next, the DV means of the posttest scores of Groups A_1 and B were compared. Similarly, the DV means of the posttest scores of Groups A_2 and B were compared. These tests had the purpose of verifying whether the treatments had any resulting effect on the respondents' behavioral intent. As shown by the results in Table 16, the t-tests results indicated there were no statistically significant differences between the groups tested. In summary, because there were no group differences found, there is no evidence of internal validity of the experimental methods.

Table 16 Independent Samples T-Tests of Posttest Data Sets

	Levine's Test		t-test for Equality of means						
								95% CI of the Difference	
Group Means Compared	**F**	**Sig**	**t**	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Std. Error Difference**	**Lower**	**Upper**
$A_1 = 4.0556$, $A_2 = 3.8333$									
Equal variances assumed	.303	.584	.853	58	.397	.2222	.26058	-.29938	.74383
Equal variances not assumed			.853	57.684	.397	.2222	.26058	-.29944	.74389
$A_1 = 4.0556$, B = 3.9333									
Equal variances assumed	.046	.831	.487	58	.628	.12222	.25092	-.38004	.62448
Equal variances not assumed			.487	58	.628	.12222	.25092	-.38004	.62448
$A_2 = 3.8333$, B = 3.9333									
Equal variances assumed	.555	.459	-.384	58	.703	-.10000	.26073	-.62192	.42192
Equal variances not assumed			-.384	57.695	.703	-.10000	.26073	-.62197	.42197

Because the results of the t-tests and ANOVA tests found no statistically significant difference between the experimental and control group posttest DV means, the null hypotheses for H11, H12, and H13 cannot be rejected and these hypotheses are not supported.

Revised Sample and Characteristics

The pretest and posttest included the same items and therefore either could be used for the remaining analyses in this dissertation. In the case where the pretest and posttest DV means were found statistically significantly different, separate analyses could be performed on the pretest and the posttest data sets. In this dissertation study, where no differences were found between the pretest data sets and the posttest data sets, no

meaningful results would be revealed by performing separate analyses. Therefore, the pretest response data was selected as the focus of the remaining analyses in this study.

The pretest response data available for analyses in Groups A_1, A_2, and B included 87, 97, and 31 cases, respectively, for a total of 215 cases. Due to the results of the t-tests on the posttest data, it was likely that the pretest data was also not significantly different between the three groups, which would support combining the data from all groups to be used for the EFA. Also, an additional 91 cases had been collected but were excluded from the analyses in this study so far because of incomplete treatment responses and or posttest responses. The pretest responses of these cases, referred to as Group P, were also likely to not be significantly different from the pretest responses of Groups A_1, A_2, and B, and the data sets could potentially be combined for examination in the remaining analyses of this study. To verify that the four groups' pretest data was not significantly different and therefore could be combined into one data set, the three independent samples t-tests that were performed on the posttest data sets were repeated on the pretest DV means of the four groups, using 30 randomly selected cases from each group. As with the posttest t-test comparisons and as shown in Table 17, no evidence was found to reject the hypothesis that the group DV means were equal; therefore Groups A_1, A_2, B, and P pretest response data sets were combined for a total of 306 cases available for all the remaining statistical analyses in this study, beginning with the EFA reported next.

Table 17 Independent Sample T-Tests of Pretest Data Sets

	Levene's Test		t-test for Equality of Means						
								95% CI of the Difference	
Group Means Compared	**F**	**Sig**	**t**	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Std. Error Difference**	**Lower**	**Upper**
$A_1 = 4.0778$, $A_2 = 3.8889$									
Equal variances assumed	2.481	.121	.725	58	.472	.18889	.26067	-.33290	.71067
Equal variances not assumed			.725	55.48	.472	.18889	.26067	-.33340	.71118
$A_1 = 4.0778$, B = 3.8889									
Equal variances assumed	.319	.574	.773	58	.443	.18889	.24449	-.30051	.67828
Equal variances not assumed			.773	57.36	.443	.18889	.24449	-.30062	.67840
$A_1 = 4.0778$, P = 3.7556									
Equal variances assumed	1.418	.239	1.264	58	.211	.32222	.25502	-.18826	.83270
Equal variances not assumed			1.264	46.22	.212	.32222	.25502	-.18860	.83305
$A_2 = 3.8889$, B = 3.8889									
Equal variances assumed	.921	.341	.000	58	1.000	.00000	.27248	-.54542	.54542
Equal variances not assumed			.000	57.31	1.000	.00000	.27248	-.54557	.54557
$A_2 = 3.8889$, P = 3.7556									
Equal variances assumed	.126	.724	.473	58	.638	.13333	.28197	-.43109	.69775
Equal variances not assumed			.473	57.92	.638	.13333	.28197	-.43110	.69777
B = 3.8889, P = 3.7556									
Equal variances assumed	.358	.552	.499	58	.620	.13333	.26708	-.40129	.66795
Equal variances not assumed			.499	57.686	.620	.13333	.26708	-.40135	.66802

The addition of the group of cases that had initially been discarded resulted in a significant change to the data set originally analyzed; therefore the sample characteristics were reexamined and are presented in Table 18. The primary difference in the new data

set was that the demographic item responses were missing for about 25% of the cases. The characteristics of the respondents with non-missing demographics were similar to the original set analyzed in this dissertation. Again, the proportion of males and females was approximately equal and the ages ranged from 18 to 79. The number of students, faculty, and staff were again nearly equally represented with a slightly larger number of faculty. The respondents reported similar levels of education as with the previous sample, with the majority at the doctoral level, followed by the master's, and then the bachelor's and the other levels represented at smaller numbers. A total of 133 respondents (43.5%) reported having at least 10 years of work experience. Those who reported at least 10 years of computing experience made up 28.4% of the sample, with 19% each reporting 3-9 years and 25 years or more. While this sample's characteristics were different from the previous sample, the large amount of missing demographic data precludes a closer examination.

Table 18 Primary Study Respondent Revised Sample Characteristics

Demographic		Count (N)	Percentage (%)
Gender	Male	111	36.3
	Female	107	35
	Missing data	88	28.7
Age	18-19	6	2.0
	20-29	50	16.3
	30-39	65	21.2
	40-49	45	14.7
	50-59	35	11.4
	60-69	13	4.2
	70-79	1	0.3
	Missing data	91	29.7
Position	Student	62	20.3
	Staff	61	19.9
	Faculty	84	27.5
	Other	14	4.6
	Missing data	85	27.8
Education	High School	6	2.0
	Some College	23	7.5
	Associate's	9	2.9
	Bachelor's	43	14.1
	Master's	67	21.9
	Doctoral	74	24.2
	Missing Data	84	27.4
Years of Computing Experience	Fewer than 3	4	1.3
	3-9	15	4.9
	10-24	133	43.5
	25 or more	70	22.9
	Missing Data	84	27.4
Years of Work Experience	Fewer than 3	19	6.2
	3-9	58	19.0
	10-24	87	28.4
	25 or more	58	19.0
	Missing data	84	27.4

As shown in Table 19, the answers to the question asked at the beginning of the survey provide evidence that the great majority of respondents (94.1%) do regularly use a

computer that stores data that they perceive to be important and that they want to protect. This supports the assumption that the surveyed population was appropriate for this study.

Table 19 Initial Question Frequency Analysis

Answers	Count (N)	Percentage (%)
Not Sure	8	2.6
Yes	288	94.1
No	10	3.3

Exploratory Factor Analyses

The factor analyses included statistical tests to enable the examination of the descriptive statistics. The sample size of the combined groups A_1, A_2, B, and P was 306, considerably more than 200 which is an acceptable size for the technique of factor analysis (Hair et al., 2010; Tabachnick & Fidell, 2007). A review of the pretest responses revealed no missing data. The items, Likert scale type with 1 being "Strongly Disagree" and 5 being "Strongly Agree," showed an acceptable response spread with minimum values of 1 and maximum values of 5 for all except the items REF2 and REF3, and VRE2 which each had a minimum of 2 and maximum of 5. No unusual means or standard deviations were noted. Skewness and kurtosis was evident but the skewness values were all less than |2.0| and kurtosis values were all less than |7.0| indicating the data were all in the range generally considered to be normal based on the Monte Carlo simulation research rule-of-thumb (Byrne, 1998, 2010). Box plots identified univariate outliers for nearly all variables. However, examination of the individual cases found that all appeared to be valid and therefore should be retained. The descriptive statistics for the data set is presented for review in Appendix C.

Statistical tests were performed to verify that the factor analysis technique was appropriate for use with the sample. The Bartlett's Test of Sphericity (Bartlett's) null hypothesis is that the correlations in the sample matrix are zero. The test is highly sensitive to sample size and therefore its result should be considered along with the results of other tests such as Kaiser-Meyer-Olkin Measure of Sampling Adequacy test (KMO) and examination of the off-diagonal elements of the anti-image correlation matrix. The KMO test produces an index value representative of the degree of variable intercorrelation. The KMO should be at a minimum of .50, and greater than .60 to indicate adequate sampling (Tabachnick & Fidell, 2007) or greater than .80 to indicate excellent sampling (Hair et al., 2010). The anti-image correlation matrix contains the values in the off-diagonal elements that are the negatives of the partial correlations that exist between the variables. Partial correlations that are greater than .70 are considered to be a statistically significant indication that the sample matrix may not be appropriate for factor analysis. As shown in Table 20, Bartlett's was significant at .000, KMO was not significant at .873, and all partial correlations in the anti-image correlation matrix were less than .70, providing evidence that the factor analysis technique is appropriate for the sample.

Table 20 Tests of Factor Analysis Appropriateness

Source	Result	Sample appropriate for factor analysis?
Bartlett's Test of Sphericity	.000	Yes
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	.873	Yes
Diagonal values in anti-image correlation matrix	All <.70	Yes

The statistical technique of Principal Components Analysis with Varimax rotation was employed. Nine factors were initially extracted based on the Eigen-value-greater-than-one rule and explained a total of 78.1% of the variance. The lowest item communality value was .590 for TSU1 which was still well above the minimum required value of .30 indicating that there was a high degree of correlation among the variables. All items loaded at 0.40 or greater on at least one factor confirming that all items should be retained (Netemeyer et al., 2003). The Self-efficacy and Direct Response Experience items loaded together on one factor, and the Vicarious Threat Experience and Vicarious Response Experience items loaded together on one factor. The measures for the remaining seven constructs loaded separately on individual factors and no cross loadings greater than 0.4 were observed. This evidence along with the *a priori* theory of the presence of eleven factors supported a repeat of the EFA with a forced extraction of eleven factors (Netemeyer et al., 2003; Tabachnick & Fidell, 2007).

The communalities of the 11-factor EFA analysis were again high, with the lowest at .702 for VTE3 and being an even higher value than the previous analysis which again indicated a high level of correlation between the variables. The total variance explained by the eleven factors increased slightly from the previous EFA to 82.385% and was much higher than the 65% that is typically considered adequate in social science research (Hair et al., 2010). Another test to assist in determining the number of factors present is the Scree test (Tabachnick & Fidell, 2007). The Scree test produces a plot of the Eigenvalues against the factors (see Figure 8) and its examination suggests the presence of 10 or 11 factors.

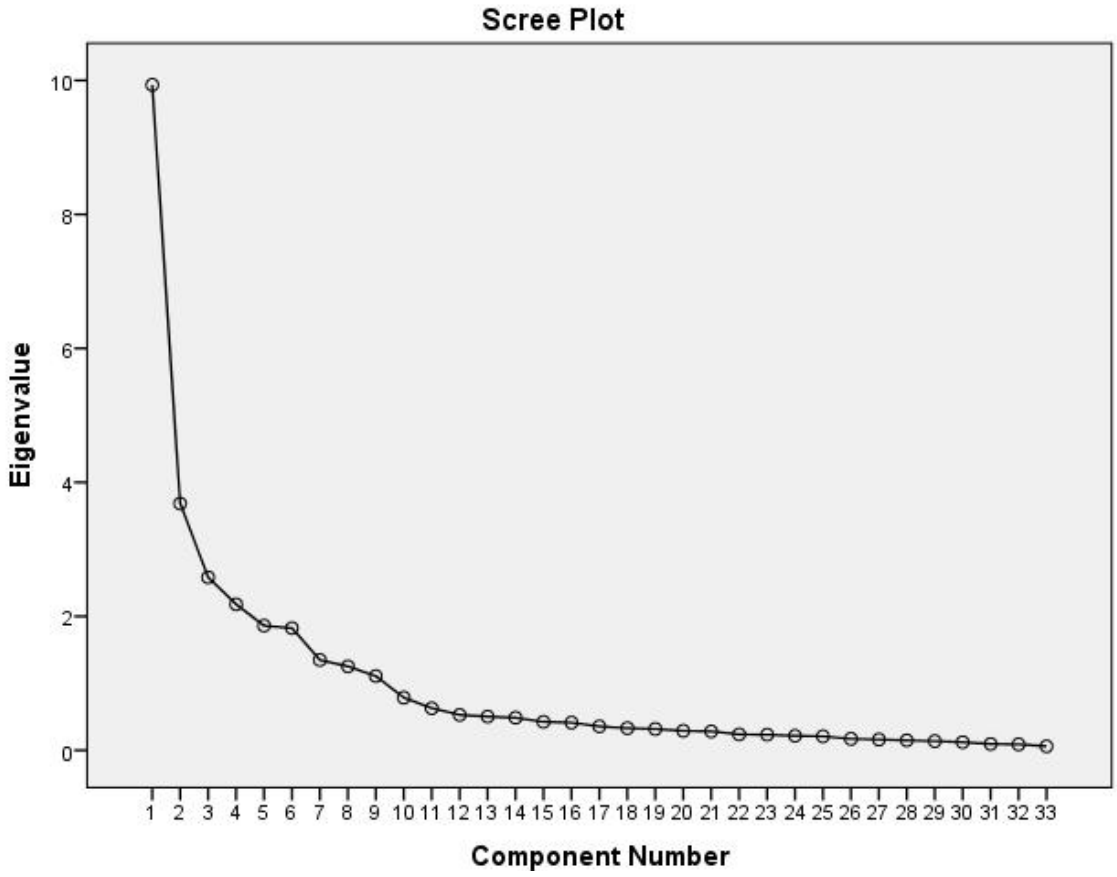

Figure 8 Scree Plot

The 11 factor rotated component matrix, presented in Table 21 with item loadings of less than .40 suppressed for ease in interpretability, shows that the Self-efficacy and Direct Response Experience items again loaded together on one factor, but the Vicarious Threat Experience and Vicarious Response Experience items were successfully separated into individual and separate factors. The Threat Susceptibility items loaded across two factors with TSU3 unable to load higher than .618 on either factor.

Table 21 Primary Study EFA Analysis with 11 Factors – Rotated Component Matrix[a]

	Component										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
TSU1										.906	
TSU2											.864
TSU3										.618	.546
TSV1					.864						
TSV2					.849						
TSV3					.856						
REF1								.780			
REF2								.809			
REF3								.866			
SEF1	.857										
SEF2	.864										
SEF3	.856										
RSC1				.859							
RSC2				.885							
RSC3				.885							
SOC1							.849				
SOC2							.887				
SOC3							.766				
DTE1		.909									
DTE2		.915									
DTE3		.880									
DRE1	.840										
DRE2	.771										
DRE3	.795										
VTE1						.846					
VTE2						.829					
VTE3						.724					
VRE1									.767		
VRE2									.617		
VRE3									.734		
BEH1			.857								
BEH2			.836								
BEH3			.843								

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

The definitions of the Self-efficacy and Direct Response Experience constructs and the wording of their measures were reviewed in an effort to determine whether they were too similar and were therefore actually measuring the same rather than separate constructs. The construct definitions were similar and certainly expected to be highly correlated. The measures were determined to be distinct and able to capture separate constructs. The strong relationship between the loadings of the two constructs suggests that they may be measuring separate dimensions of another construct. Further investigation would need to be performed to gather evidence and test that proposition. Because the experience construct measures had not been tested previously, it was determined to retain both sets of measures in the model, but to accept that they would be highly correlated. A 10-factor EFA solution was run and the measures of all the constructs except for Self-efficacy and Direct Response Experience loaded on separate factors.

An examination of the 10-factor solution was performed and it was found that the VRE2 item did not load high with VRE1 and VRE3 (see table in Appendix C). The more serious issue was that VRE2 cross loaded at .432 with the vicarious threat experience construct. The wording of the VRE2 measure was examined and it was determined that it may have been awkwardly phrased and or it was unclear and should be revised to ensure that it is truly reflective of the vicarious response experience construct prior to any future tests. The VRE2 item was dropped and the EFA again run. The final 10-factor solution is shown in Table 22. While the item TSU2 did not load above .70, there was no serious cross-loading; therefore, TSU2 was retained in order to include the accepted minimum of three measurement items for the construct Threat Susceptibility (Hair et al., 2010).

Table 22 Final 10-Factor EFA Analysis Rotated Component Matrix[a]

	Component									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
TSU1									.810	
TSU2									.668	
TSU3									.834	
TSV1				.863						
TSV2				.850						
TSV3				.856						
REF1								.782		
REF2								.810		
REF3								.866		
SEF1	.860									
SEF2	.866									
SEF3	.860									
RSC1					.851					
RSC2					.886					
RSC3					.877					
SOC1							.851			
SOC2							.888			
SOC3							.765			
DTE1		.907								
DTE2		.915								
DTE3		.878								
DRE1	.844									
DRE2	.776									
DRE3	.801									
VTE1						.850				
VTE2						.837				
VTE3						.718				
VRE1										.733
VRE3										.720
BEH1			.854							
BEH2			.832							
BEH3			.847							

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

Item factor loadings should be assessed for both practical and statistical significance (Hair et al., 2010). Factor loadings of at least .50 are considered to be of practical significance, but those of .70 or more are considered to be better able to reveal well-defined factor structures. The preferred threshold for factor analysis interpretation that is practically significant is therefore considered to be .70 and above. As shown in Table 22, all of the factor loadings are greater than .70 with one exception. The factor loading for TSU2 is .668 which is very near to .70 and was deemed acceptable for this dissertation study.

The statistical significance of a factor loading is assessed more strictly than practical significance and is also related to the size of the sample to compensate for the large standard errors that are typically present with factor loadings. For a sample size of 307, as in this dissertation study, statistical significance is achieved with factor loadings of at least .35 (Hair et al., 2010). Again referring to Table 22, all of the items' factor loadings were found to be at least .35 and are therefore statistically significant.

The results of the EFA indicate that all but one of the measurement items (VRE2) were significant and should be retained. After reviewing the construct definitions it was not surprising that the Self-efficacy and Direct Response Experience measures were highly correlated; therefore, it was proposed that they may be individual dimensions of a multidimensional construct and would be allowed to correlate in this dissertation study. With this caveat in mind, the summary of the EFA results is that all other measures reflect the constructs they were expected to reflect, the measures' factor loadings are at a level to indicate they represent well-defined constructs, and evidence of convergent and discriminant validity for all construct measures was found.

Reliability Analysis

The internal reliability and consistency assessment of the measurement scales being used was performed next. Cronbach's Alpha is the most commonly used reliability assessment method (Churchill & Peter, 1984; Peter, 1979; Peterson, 1994) with the lower acceptable reliability limit being a value of .70 and values of .80 or above considered to be evidence of good reliability (Clark & Watson, 1995; Hair et al., 2010; Netemeyer et al., 2003). The mean inter-item correlations are examined to assess the internal consistency of the scales with good internal consistency demonstrated by value ranges of 0.15 to 0.25 for "higher-order" constructs and of 0.40 to 0.50 for the "narrower" constructs (Clark & Watson, 1995). An alternative rule-of-thumb states that value ranges of 0.20 to 0.29 represent "extensive evidence" and greater than 0.30 for "exemplary evidence" (Netemeyer et al., 2003; Robinson, Shaver, & Wrightsman, 1991). The Cronbach's Alpha values calculated for each scale in this dissertation study are shown in Table 23 along with the inter-item correlation value ranges found within each scale.

Table 23 Primary Study Reliability Analysis Results

	Construct	Cronbach's Alpha	Average inter-item correlations range
TSU	Threat Susceptibility	.721	.378 to .532
TSV	Threat Severity	.879	.698 to .718
REF	Response Efficacy	.846	.614 to .686
SEF	Self-efficacy	.925	.791 to .837
RSC	Response Cost	.874	.673 to .742
SOC	Social Influence	.849	.559 to .777
DTE	Direct Threat Experience	.950	.852 to .880
DRE	Direct Response Experience	.920	.737 to .840
VTE	Vicarious Threat Experience	.855	.613 to .770
VRE	Vicarious Response Experience	.773	.631
BEH	Behavioral Intent	.962	.883 to .899

The Cronbach's Alpha values are greater than .80 for all scales except Threat Susceptibility and Vicarious Response Experience which are each less than .80 but still above .70. The average inter-item correlations are all above the exemplary threshold of .30. Therefore, evidence was found of acceptable reliability for all scales.

The reliability and consistency assessment of a measurement scale may befit from the item-to-total statistics that are commonly reported as a part of the internal reliability and consistency analysis. Because evidence of acceptable internal reliability and consistency has been found, the additional information provided by the item-to-total statistics is not necessarily needed. However, because the measurement items for the self-efficacy and direct response experience constructs loaded on the same factor, these additional statistics are shown in Table 24 and a brief review was conducted.

Table 24 Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item deleted
TSU = Threat Susceptibility					
TSU1	6.96	2.890	.515	.299	.666
TSU2	7.18	2.843	.500	.275	.688
TSU3	6.48	3.083	.627	.394	.549
TSV = Threat Severity					
TSV1	8.19	2.897	.766	.587	.829
TSV2	8.08	3.125	.774	.599	.822
TSV3	8.07	3.078	.759	.576	.834
REF = Response Efficacy					
REF1	8.72	1.388	.685	.472	.813
REF2	8.69	1.409	.715	.521	.783
REF3	8.68	1.433	.740	.551	.761
SEF = Self-efficacy					
SEF1	8.34	3.319	.867	.754	.883
SEF2	8.30	3.530	.831	.691	.912
SEF3	8.26	3.387	.858	.741	.890
RSC = Response cost					
RSC1	6.42	4.402	.724	.524	.851
RSC2	6.61	4.179	.777	.609	.804
RSC3	6.64	3.989	.772	.604	.808
SOC = Social influence					
SOC1	7.55	2.865	.747	.614	.762
SOC2	7.48	2.913	.794	.651	.714
SOC3	7.28	3.540	.623	.396	.874
DTE = Direct Threat Experience					
DTE1	7.31	5.276	.897	.808	.926
DTE2	7.34	5.109	.905	.820	.920
DTE3	7.30	5.246	.884	.781	.936
DRE = Direct Response Experience					
DRE1	8.12	4.028	.882	.781	.849
DRE2	8.03	4.222	.803	.659	.913
DRE3	8.13	4.123	.830	.717	.891
VTE = Vicarious Threat Experience					
VTE1	8.42	2.073	.766	.624	.763
VTE2	8.40	1.997	.769	.628	.758
VTE3	8.55	2.065	.654	.428	.870
VRE = Vicarious Response Experience					
VRE1	4.12	.703	.631	.398	NA*
VRE3	4.29	.661	.631	.398	NA*
BEH = Behavioral Intent					
BEH1	7.52	5.313	.926	.858	.937
BEH2	7.54	5.161	.914	.837	.947
BEH3	7.49	5.365	.914	.838	.946

*NA = Not Applicable

A comparison was made of the Cronbach's Alpha values in Table 23 with the Cronbach's Alpha if Item Deleted values in Table 24 for each of the constructs. The comparison revealed that the Social Influence Cronbach's Alpha value would increase to .874 if the item SOC3 was removed. The comparison also found that the Vicarious Threat Experience Cronbach's Alpha value would increase to .870 if the item VTE3 was removed. The decision was made to retain both SOC3 and VTE3 because the Cronbach's Alpha values were already quite acceptable and more importantly because a latent variable scale should include a minimum of three measurement items whenever possible (Hair et al., 2010).

Next, the corrected item-to-total correlations were examined. This statistic represents the extent to which any one item is correlated with the other items within a measurement scale. In the early stages of scale development, the standard rule-of-thumb is to retain those items with an item-to-total correlation of .35 or more (Bearden, Hardesty, & Rose, 2001). For scales validated through previous research such as most of the scales used in this research, a stricter recommendation should be followed where items are retained only if they achieve an item-to-total correlation of at least .50 (Netemeyer et al., 2003). Any items with low correlations or that correlate more highly with items within a scale other than the scale intended should be deleted.

As is seen by the values reported in Table 24, the item-to-total correlations of all of the measures, including the four new experience items, are all above the stricter .50 value. This lends additional support to retain all remaining measurement items in each scale. In summary, there is evidence to indicate the measurement scales have acceptable internal reliability and consistency.

Confirmatory Factor Analysis

The analysis continued with a confirmatory factor analysis (CFA) which was conducted using the statistical technique of structured equation modeling (SEM) with the software package IBM SPSS Amos version 20. The technique of SEM enables simultaneous analyses of both the measurement and the predictive (structural) models through construct relationship examination while accounting for the measurement error, making the technique confirmatory (Kelloway, 1998; Tabachnick & Fidell, 2007). A two-step approach was used (Anderson & Gerbing, 1988) with examination of the measurement model performed first in order to establish evidence of reliability, and convergent and discriminant validity. After the measurement model was assessed, the structural model assessment was performed to establish predictive validity.

Measurement Model Evaluation

Assessment of a measurement model with the techniques of SEM is primarily achieved by reviewing the model fit which is determined by the level of adequacy of the parameter estimates and by the overall model fit which is determined by review of a series of fit statistics (Byrne, 2010). SEM relies on the assumption of normality of the data sample. Examination of the skewness and kurtosis of a distribution is commonly performed to assess normality. Furthermore, a sample with positive kurtosis is known to influence tests of variance and covariance (Byrne, 2010; Tabachnick & Fidell, 2007). Because the SEM technique is based on the analyses of covariance structures, kurtosis is of particular concern. Therefore, the model evaluation began with reviewing the normality assessment output with a focus on kurtosis.

The normality assessment results provided by the IBM SPSS Amos software (see Appendix C) included univariate and multivariate kurtosis statistics. The univariate

kurtosis threshold commonly considered to be an acceptable indication of normality is $\leq |7|$ (Byrne, 1998, 2010). The results of the normality assessment revealed univariate kurtosis values ranging from -.916 to 3.788, well below the acceptable threshold value. Therefore no indication of univariate kurtosis was evident and the assumption of univariate normality was supported. The multivariate kurtosis statistic provided by the normality assessment was 400.427 with a critical ratio (C.R.) of 75.080. Non-normal distributions are indicated by C.R. values > 5.0 (Bentler, 2005). Therefore, evidence of multivariate non-normality is present. When the data sample is multivariate non-normal, the results of an SEM analysis using maximum likelihood (ML) estimation may require adjusted interpretations. An alternate estimation available is asymptotic distribution-free (ADF); however this estimation method requires very large sample sizes. The current study included a sample size of 308 with 162 parameters being estimated. Because the sample size is considered too small for the ADF estimation method, and because the effects of kurtosis on variance and covariance tests has been found to be minimized in sample sizes >200 (Tabachnick & Fidell, 2007), the analysis continued using the ML estimation method.

A review of the multivariate outliers also provided by IBM SPSS Amos software output was performed next. The Mahalanobis distance (D^2) statistic for each case was examined, and a portion of the output is reproduced in Appendix C. Several cases were identified as potential outliers, but a closer examination determined that the evidence was not definitive and that the cases may instead be representative of the population. Therefore, without stronger evidence of outliers, no cases were removed.

The estimates and each corresponding C.R. values were reviewed. The factor loadings and variances were all found to be statistically significant at the $p<.001$ level.

Error variances were all at acceptable values as well. The measurement model listing the standardized factor loadings, item SMC values, and correlations is shown in Figure 9. Table 25 presents both unstandardized and standardized factor loadings, the approximate standard error (S.E.), and the C.R. values for each measure.

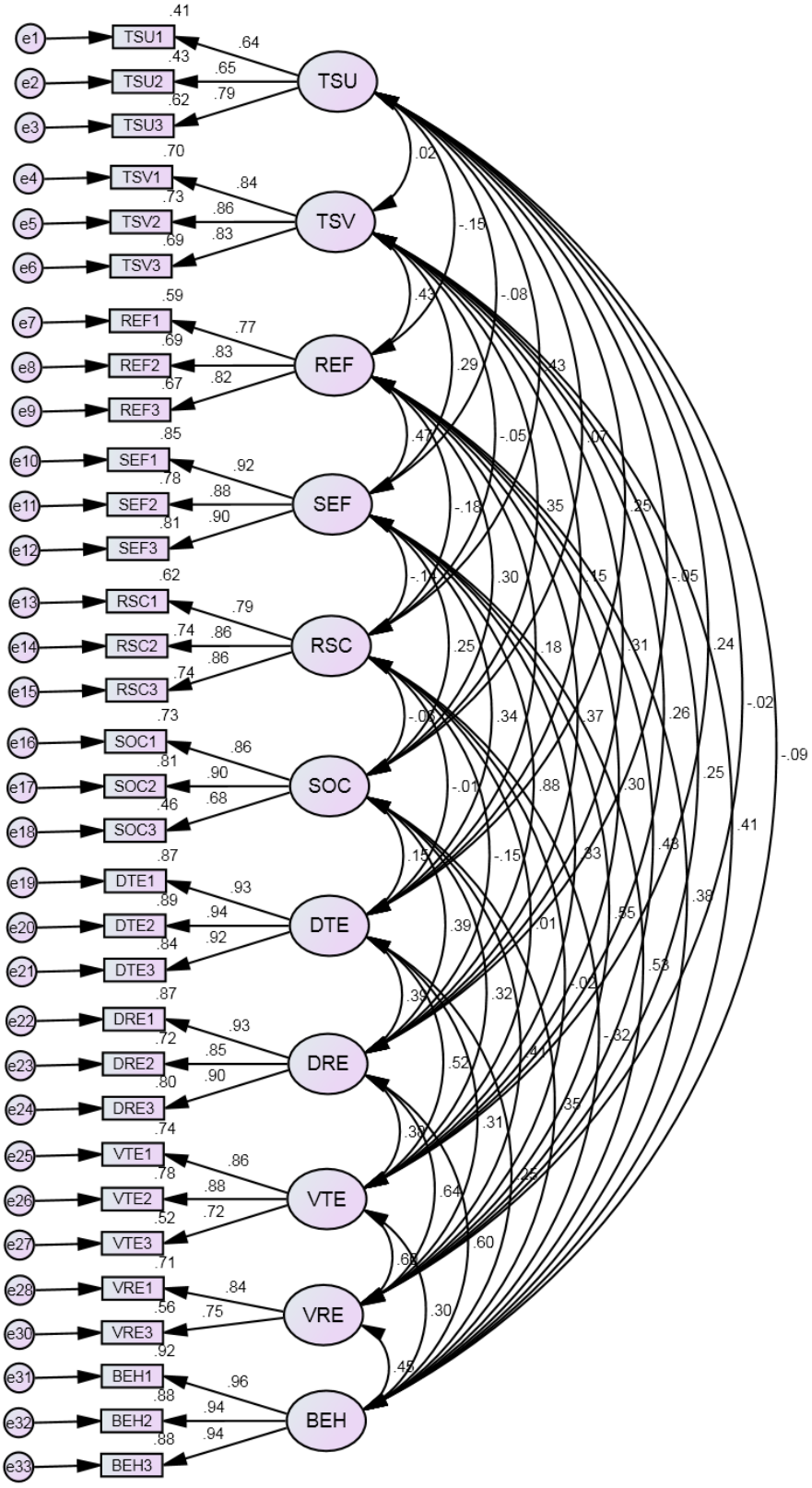

Figure 9 Measurement Model with Standardized Estimates

Table 25 Measurement Model Parameter Estimates

Relationship	Standardized Estimate	Unstandardized Estimate	S.E.	C.R.	p
TSU→TSU1	0.643	0.968	0.104	9.300	***
TSU→TSU2	0.653	1.010	0.116	8.737	***
TSU→TSU3	0.786	1			
TSV→TSV1	0.839	1.066	0.065	16.287	***
TSV→TSV2	0.856	1.003	0.061	16.430	***
TSV→TSV3	0.830	1			
REF→REF1	0.769	1.011	0.073	13.884	***
REF→REF2	0.829	1.049	0.071	14.750	***
REF→REF3	0.819	1			
SEF→SEF1	0.921	1.039	0.041	25.478	***
SEF→SEF2	0.881	0.959	0.042	22.768	***
SEF→SEF3	0.899	1			
RSC→RSC1	0.787	0.861	0.056	15.391	***
RSC→RSC2	0.859	0.951	0.056	16.843	***
RSC→RSC3	0.861	1			
SOC→SOC1	0.857	1.421	0.112	12.703	***
SOC→SOC2	0.901	1.422	0.108	13.108	***
SOC→SOC3	0.679	1			
DTE→DTE1	0.931	0.999	0.036	28.131	***
DTE→DTE2	0.941	1.038	0.036	28.949	***
DTE→DTE3	0.918	1			
DRE→DRE1	0.934	1.027	0.039	26.068	***
DRE→DRE2	0.850	0.944	0.045	20.878	***
DRE→DRE3	0.896	1			
VTE→VTE1	0.861	1.087	0.078	13.952	***
VTE→VTE2	0.882	1.154	0.083	13.986	***
VTE→VTE3	0.721	1			
VRE→VRE1	0.840	1.085	0.094	11.500	***
VRE→VRE3	0.751	1			
BEH→BEH1	0.957	1.020	0.029	34.707	***
BEH→BEH2	0.940	1.040	0.032	32.505	***
BEH→BEH3	0.939	1			

***Significant at the p<.001 level.

Evidence of convergent validity was gathered through an examination of the loadings between the constructs and the construct measurement items. Factor loading values greater than or equal to 0.7 are evidence of convergent validity (Hair et al., 2010).

Twenty-nine of the thirty-two standardized loading estimates were found to be greater than .7. The three estimates below .7 were TSU1, TSU2, and SOC3 and the loadings were at .643, .653, and.679 respectively, which are very near to .7 and therefore all of the factor loadings were considered acceptable for this study.

The squared multiple correlations (SMC) for each item should be examined for evidence of reliability at the item level. The SMC represents the percentage of variance in the item being accounted for by the construct. SMC values should be .5 or greater, with lower values being evidence that the item is not a good reflection of the construct and therefore is an indication of poor model fit (Hair et al., 2010).

Twenty-nine of the thirty-two SMC values, listed in Table 26, meet the minimum acceptable .5 threshold value. The SMC values for TSU1, TSU2, and SOC3 were just below the preferred .5 value at .413, .426, and .461 respectively. This indicates that future use of these three items should be preceded by closer examination and possibly a revision to ensure improved item-level reliability.

Table 26 Measurement Model Reliability

Item	SMC: Item Level Reliability	Construct	AVE: Construct Level Reliability
TSU1	0.413	TSU	.485
TSU2	0.426		
TSU3	0.617		
TSV1	0.703	TSV	.708
TSV2	0.733		
TSV3	0.689		
REF1	0.591	REF	.650
REF2	0.687		
REF3	0.672		
SEF1	0.849	SEF	.811
SEF2	0.777		
SEF3	0.808		
RSC1	0.619	RSC	.699
RSC2	0.738		
RSC3	0.741		
SOC1	0.735	SOC	.669
SOC2	0.812		
SOC3	0.461		
DTE1	0.867	DTE	.865
DTE2	0.886		
DTE3	0.842		
DRE1	0.872	DRE	.799
DRE2	0.722		
DRE3	0.803		
VTE1	0.741	VTE	.680
VTE2	0.778		
VTE3	0.520		
VRE1	0.706	VRE	.635
VRE3	0.564		
BEH1	0.915	BEH	.893
BEH2	0.883		
BEH3	0.882		

Each construct's Average Variance Extracted (AVE), an indicator of reliability at the construct level, is shown in Table 26 with the SMC values. The AVE is calculated by dividing the sum of the item SMC values by the number of items and therefore represents

the average percentage of variance among a set of measures that is accounted for by the construct they are attempting to measure in the model. The accepted threshold value is .50 or more for good fit (Fornell & Larcker, 1981; Garver & Mentzer, 1999; Hair et al., 2010; Hu & Bentler, 1995). The AVEs for all constructs met the minimum accepted value of .50 with the exception of one construct, threat susceptibility (TSU), which was just under the preferred threshold value at .485. This is not surprising because the SMC values of two of the three item measures for threat susceptibility were also under the preferred threshold value. However, this value is near the desired threshold and the construct is a core construct in the model; therefore the reliability was deemed acceptable.

Evidence of discriminant validity at the item level is gathered by an examination of the modification indices (MI) of the factor loadings. MI values greater than 5 between construct measurement items and other constructs are indicators of possible cross loading and therefore evidence of poor discriminant validity at the item level. Two factor loading MI values exceeded 10. One MI was 14.161 and was between DTE3 and the construct direct response experience. The other MI value was 11.129 and was between DTE3 and self-efficacy. This suggests that the measure DTE3 not only measures direct threat experience, but also cross loads with direct response experience and self-efficacy, and does not exhibit discriminant validity as clearly as the other measures. There were no other large MI values and therefore the discriminant validity at the item level was acceptable for this model.

The fit statistics of the measurement model were examined and are shown in Table 27 along with the commonly recommended threshold value for each. The Chi-square statistic should be statistically non-significant, and the statistic Chi-square Index,

calculated by dividing the Chi-square value by the degrees of freedom, should be between 3.0 and 5.0 (Kelloway, 1998). The more rigorous rule of thumb value for the Chi-square Index is a value of <3.0 (Carmines & McIver, 1981). Other statistics reviewed included the Goodness of Fit (GFI), Adjusted Goodness of Fit (AGFI) and the Normed Fit Index (NFI) should be ≥0.90 (Bentler & Bonett, 1980; Chin & Todd, 1995). A Comparative Fit Index (CFI) value of ≥0.90 was also originally considered to be an indication of good model fit since revised to a more rigorous value of ≥0.95 (Hu & Bentler, 1999). Other fit indices include the Root Mean Square Error of Approximation (RMSEA) of ≤.08 (Browne & Cudeck, 1993), or the more rigorous value of ≤ 0.06 (Hu & Bentler, 1999), and the Root Mean Square Residual (RMR) ≤0.08 (Browne & Cudeck, 1993).

Table 27 Measurement Model Statistics

Statistic	Recommended Value	Calculated Value
Chi-square Statistic	--	654.370
Degrees of freedom (df)	--	409
Chi-square Statistic significance	--	.000
Chi-square Index (Chi-square/df)	<3	1.600
Root Mean Squared Residual (RMR)	≤.08	.036
Goodness of Fit (GFI)	>.90	.887
Adjusted Goodness of Fit (AGFI)	>.90	.854
Normed Fit Index (NFI)	>.90	.916
Comparative Fit Index (CFI)	>.95	.966
Root Mean Square Error of Approximation (RMSEA)	≤.08 / ≤.06	.044

The Chi-square Statistic was significant; however, this statistic is highly sensitive to sample size and is therefore likely to result in a significant result when the sample is large as was the sample in this study (Byrne, 2010; Kelloway, 1998). The CFI and the

RMSEA are considered to be two of the most useful fit statistics (Byrne, 2010). The NFI, considered as the recommended fit statistic of choice throughout the 1980's, was replaced by the CFI because it additionally accounts for sample size. The RMSEA is sensitive to model complexity and is therefore considered to be a highly informative fit statistic. The CFI at .966 is above the recommended value of .95, and the RMSEA value at .044 is well below the more rigorous recommended value of .06. Even with the GFI at .887 and the AGFI is at .854, values just under the recommended threshold, the majority of the fit statistics indicate a very good model fit.

The standardized residuals and the modification indices were reviewed to detect the existence of model misspecification. Standardized residual values greater than $|2.58|$ are an indication of potential model misspecification. The standardized residual covariance matrix was reviewed and all residuals were within acceptable values. Modification indices (MI) with values greater than 5.0 are considered to be model misspecification indicators. A more practical MI level of 10.0 may be used to identify potential areas to consider re-specification of the model (Byrne, 2010). High covariance MI values between error terms within constructs may be evidence of systematic errors. No large MI covariance values were found between the within construct error terms. The conclusion made from these findings was that the model was not misspecified.

In summary, the assessment of the measurement model identified evidence of overall reliability, and convergent and discriminant validity. Issues discovered, however, included the indication that two of the constructs, Self-efficacy and Direct Response Experience, were highly correlated. Furthermore, it was proposed in this dissertation that Self-efficacy and Direct Response Experience may be separate dimensions of a multidimensional construct. The analyses of the structural model using the technique of

SEM revealed possible cross-loadings between the item DTE3 and the constructs direct response experience and self-efficacy as indicated by factor loading MI values >10. If the evidence of cross-loading had been more severe, DTE3 would have been removed from the model. However, because the evidence found was not particularly strong, and because this study is the first test of the Direct Threat Experience and the other three experience constructs, it was determined that no changes to the measurement model were necessary.

Tests for Common Method Bias

During the development phase of the instrument, a focused attempt was made to exclude ambiguity, duality, or any other potentially confusing characteristics within the measures in order to reduce common method bias (Podsakoff et al., 2003). During the data collection phase, the study participants were given assurances of anonymity to encourage honesty in the responses given and thereby reduce common method bias. To verify no significant biases were introduced by the method of the data collection or by the instrument or its measures, statistical tests were performed (Gaskin, 2011a; Podsakoff et al., 2003) before continuing with the remaining analyses. Two different tests were conducted; the first was the Harman's single factor test that was performed using IBM SPSS Statistics version 20, and the second was the Common Latent Factor test performed using IBM SPSS Amos version 20.

The Harman's single factor test was performed by performing an EFA with all of the factors in the model, no rotation, and with the model constrained to a single factor. While the test does not indicate the source of the bias (Podsakoff et al., 2003), a single factor in a model that explains more than 50% of the variance in the model represents

evidence of serious common method bias (Gaskin, 2011a). The total variance extracted by the single factor in this study was 28.30% which indicates that common method bias exists but the strength of the bias is low.

The Common Latent Factor test was performed next. A single variable called Common was added to the measurement model. The specific identification of the variable Common is not necessary (Podsakoff et al., 2003) as it simply represents an unknown variable with which the variables in the model may share a common variance. The variance of Common was set to be equal to 1, and regression lines were drawn from Common to each of the observed variables. The regression lines weights were constrained to be equal to each other and to a variable, c. The model was run using the software and the regression weight of the variable c was calculated to be equal to .35. To calculate the common variance of the model, the regression weight value of .35 was squared. The common variance of the model was found to be equal to about 12%, a result well below 50%, again indicating the existence of common method bias but at a level considered to be low (Gaskin, 2011a). Because both of the statistical tests indicated that the common method bias was not particularly serious, the study continued with the remaining analyses of the dissertation, beginning with the assessment of the structural model.

Structural Model Evaluation

After the examination of the measurement model confirmed that the measures were adequate and that the model was a good fit to the data, the examination of the structural model was performed to establish predictive validity. This included a review

of the model fit statistics and of the magnitude and direction of the relationships between constructs.

The Chi-square Index, RMR, CFI, and RMSEA were again found to be at the preferred values as shown in Table 28. As with the measurement model, GFI, AGFI, and NFI were just under the preferred thresholds, but the evidence indicated a the structural model was also a good fit to the data.

Table 28 Structural Model Fit Statistics

Statistic	Recommended Value	Calculated Value
Chi-square Statistic	--	781.885
Degrees of freedom (df)	--	434
Chi-square Statistic significance	--	.000
Chi-square Index (Chi-square/df)	<3	1.802
Root Mean Squared Residual (RMR)	≤.08	.076
Goodness of Fit (GFI)	>.90	.869
Adjusted Goodness of Fit (AGFI)	>.90	.840
Normed Fit Index (NFI)	>.90	.899
Comparative Fit Index (CFI)	>.90	.952
Root Mean Square Error of Approximation (RMSEA)	≤.08 / ≤.06	.051

The structural parameter estimates, presented in Table 29, were examined in order to evaluate Hypotheses 1a-10. Eleven of the 20 paths were found to be statistically significant. Six of the 11 significant paths were found to be indicators of very strong relationships, with the estimates produced found to be significant at the <.001 level.

Table 29 Structural Parameter Estimates

Relationship	Standardized Estimate	S.E.	C.R.	p
TSV→BEH	.220	.077	3.973	***
TSV→REF	.331	.041	5.276	***
TSV→SEF	.037	.041	1.017	.309
TSU→BEH	.043	.080	.803	.422
TSU→REF	-.164	.046	-2.512	.012*
TSU→SEF	-.049	.047	-1.265	.206
REF→BEH	.052	.126	.880	.379
SEF→BEH	.405	.068	7.327	***
RSC→BEH	-.254	.055	-5.035	***
DRE→REF	.125	.043	1.524	.127
DRE→SEF	.899	.053	15.053	***
DRE→RSC	-.224	.090	-2.511	.012*
VRE→SEF	-.016	.074	-.292	.770
VRE→REF	.288	.072	3.190	.001**
VRE→RSC	.108	.147	1.146	.252
DTE→TSV	.018	.052	.246	.805
DTE→TSU	.177	.052	2.228	.026*
VTE→TSV	.267	.102	3.426	***
VTE→TSU	.125	.099	1.522	.128
SOC→BEH	.141	.093	2.654	.008**

*Significant at the p<.05 level
**Significant at the p<.01 level
***Significant at the p<.001 level

The structural model is illustrated in Figure 10 and includes the path estimates with notable construct SMC values. This visual representation of the predictions tested shows that the primary predictors of behavioral intent were threat severity, self-efficacy, response cost, and social influence, with threat susceptibility and response efficacy contributing very little to the predictive power of the model. Additionally, it can be seen that direct threat experience, vicarious threat experience, direct response experience, and vicarious response experience are important additions to the traditional PMT model, particularly by the extremely high estimate value of .899 in the predictive path of direct response experience to self-efficacy.

Examination of the construct SMC values reveals that 79.1% of the variance in self-efficacy is explained by direct response experience, threat susceptibility, and threat severity, with direct response experience explaining the majority of the variance. Also shown by Figure 10 is that 29.8% of the variance of response efficacy is being explained, in order of importance, by threat severity, vicarious response experience, threat susceptibility, and direct response experience. The final notable SMC value is that of behavioral intent, which has 42.9% of its variance being explained by the model.

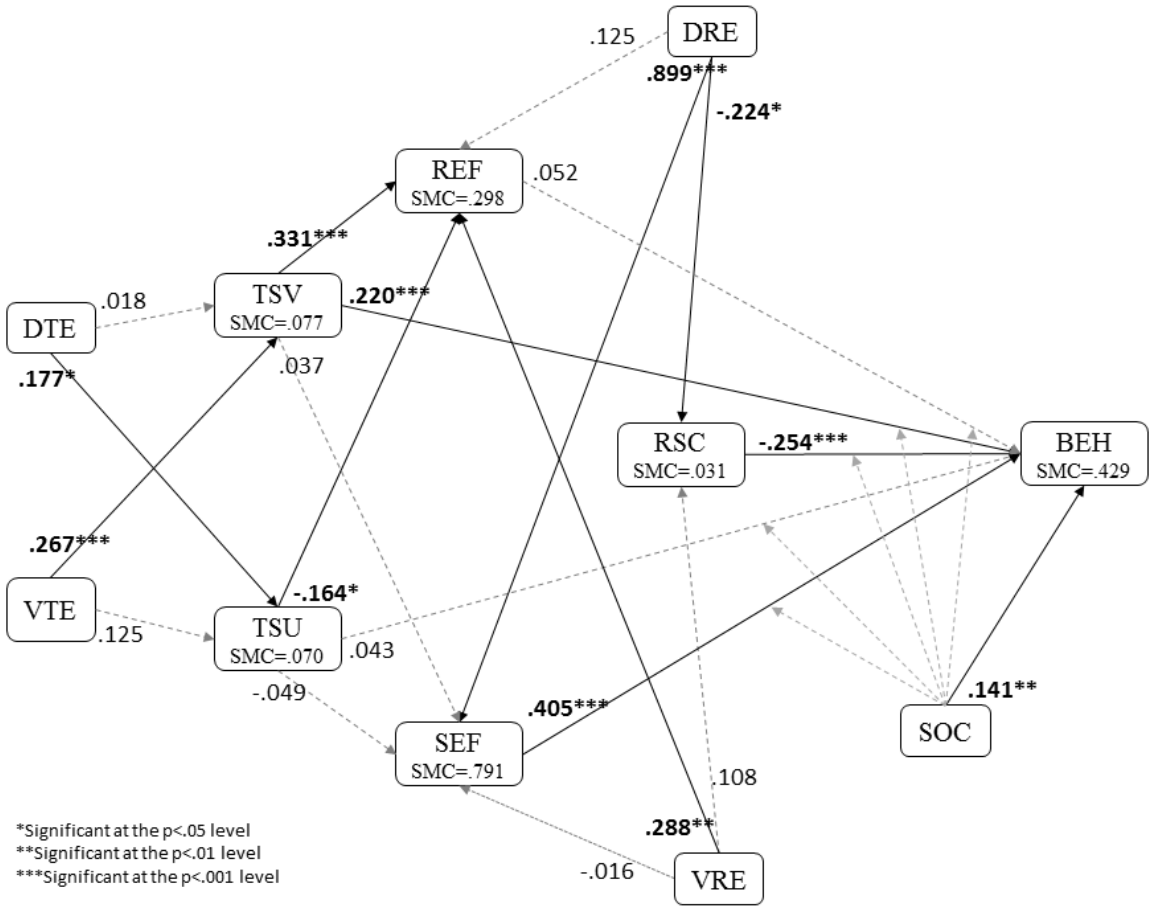

Figure 10 Structural Model with Standardized Estimates

The final analysis on the structural model included tests for the existence of moderating effects by social influence on the relationships between each of the IVs threat severity, threat susceptibility, response efficacy, and self-efficacy, and the DV behavioral intent. The statistical analysis method used to test for moderation is dependent upon the type of variables in the study (Baron & Kenny, 1986). For a study such as this dissertation that involves latent variables, there are two methods typically used to test for moderation effects (Gaskin, 2011b, 2012b). One method treats the moderating variable as dichotomous with dummy variables created for a high level and for a low level. A group analysis is then performed to test for differences between the two groups. The

other method is to test for a joint effect of the IV and the moderator on the DV. This is operationalized by creating a new interaction variable equivalent to the product of the IV and the moderator and the interaction variable is then included in the SEM analysis. No consensus exists in the literature as to which method is superior; therefore, both methods were performed.

The group comparison test was conducted first. The groups were formed by creating a dummy dichotomous variable to split the sample into a high (HiSOC) and a low (LoSOC) social influence group. The mean of the observed social influence measures was calculated to be 3.718 and used as the cutoff to separate cases into HiSOC or LoSOC. The values assigned to the dummy variable were 1=HiSOC and 2=LoSOC. A group SEM analysis was run first with the hypothesized model and then again with a fully constrained model with all paths set equal to each other. The analyses were run with the Critical Ratios for Differences output option selected in IBM SPSS Amos. This produced a matrix output that contained the C.R values for the difference comparisons of each parameter estimate pair in the model in both groups. The matrix output along with the parameter estimates from each group were input into an Excel statistical tool (Gaskin, 2012a) which provided parameter estimates with z-scores for each of the model paths. As shown by the results in Table 30, no evidence of moderation by social influence was found.

Table 30 Results of Moderation Group Comparison Tests

	HiSOC		LoSOC		
Model Path	**Estimate**	**p**	**Estimate**	**p**	**z-score**
TSV→BEH	.168	.212	.383	.000	1.312
TSU→BEH	-.035	.730	.176	.157	1.313
REF→BEH	-.097	.647	0.131	.410	.862
SEF→BEH	.388	.002	.512	.000	.807
RSC→BEH	-.281	.000	-.290	.000	-.085

The interaction method to test for moderation was conducted next. The first step was to revisit the data set in IBM SPSS and save the standardized values for all of the variables in the structural model. Standardized variables were used to remove any potential multicollinearity that may result from use of the interaction variables in the SEM analysis. Next, the interaction variables were created which was achieved by multiplying each standardized item measure of threat susceptibility, threat severity, response efficacy, self-efficacy, and response cost by the standardized item measures of social influence. For example, the standardized item measures of threat susceptibility (ZTSU1, ZTSU2, and ZTSU3) were each multiplied by the standardized item measures of SOC (ZSOC1, ZSOC2 and ZSOC3). This created nine new item measures for the new unobserved interaction variable of zTSUzSOC.

Ztsu1Zsoc1=ZTSU1 * ZSOC1
Ztsu1Zsoc2=ZTSU1 * ZSOC2
. . .
Ztsu3Zsoc2=ZTSU3 * ZSOC2
Ztsu3Zsoc3=ZTSU3 * ZSOC3

The standardized item measures were used to replace all of the item measures in the structural model. The five additional interaction variables were added as exogenous variables and paths were drawn from each to the standardized behavioral intent (zBEH) variable. The analysis was run, and the estimates were reviewed. The interaction

variable path estimates were examined first and the least significant path was removed from the model. The analysis was run again and the interaction variable path estimates reviewed. The model trimming continued in an iterative manner, examining the interaction paths first and removing the least significant path. The hope was that at some point during the model trimming process, all the interaction paths that remained would be significant, but this did not occur. The iterative path removal process resulted in all of the interaction paths being selected for removal at which time the trimming process ceased. The details of the model trimming process are presented in Table 31. The path between the standardized threat severity-social influence interaction variable and the standardized behavioral intent dependent variable being the last path removed prior to discontinuing the model trimming process.

Table 31 Structural Model with Interaction Paths - Iterative Removal Details

Relationship	Estimate	S.E.	C.R.	p	Comment
zTSUzSOC→zBEH	-.023	.051	-.457	.648	Removed 2nd, value at removal
zTSVzSOC→zBEH	-.078	.052	-1.504	.133	Removed 5th, value at removal
zREFzSOC→zBEH	.009	.097	.088	.930	Removed 1st, value at removal
zSEFzSOC→zBEH	.063	.049	1.303	.193	Removed 4th, value at removal
zRSCzSOC→zBEH	.097	.062	1.564	.118	Removed 3rd, value at removal
zTSV→zBEH	.243	.062	3.936	***	Final values after iterative path removals
zTSV→zREF	.319	.06	5.278	***	
zTSV→zSEF	.041	.039	1.065	.287	
zTSU→zBEH	.049	.061	.814	.416	
zTSU→zREF	-.162	.064	-2.524	.012	
zTSU→zSEF	-.056	.042	-1.313	.189	
zREF→zBEH	.062	.068	.910	.363	
zSEF→zBEH	.418	.057	7.317	***	
zRSC→zBEH	-.275	.054	-5.051	***	
zDRE→zREF	.099	.072	1.38	.168	
zDRE→zSEF	.893	.058	15.285	***	
zDRE→zRSC	-.185	.084	-2.21	.027	
zVRE→zSEF	-.026	.063	-.406	.685	
zVRE→zREF	.331	.096	3.449	***	
zVRE→zRSC	.083	.107	.78	.435	
zDTE→zTSV	.014	.066	.209	.834	
zDTE→zTSU	.157	.070	2.236	.025	
zVTE→zTSV	.313	.090	3.475	***	
zVTE→zTSU	.141	.093	1.523	.128	
zSOC→zBEH	.194	.072	2.693	.007	

Both moderation test methods found no evidence that Social Influence exhibited any moderating effects on the relationships between the IVs threat severity, threat susceptibility, response efficacy, and self-efficacy, and the DV behavioral intent. The lack of evidence of moderation indicates there is no evidence to reject the null hypotheses of Hypotheses 11a-11e and the five hypotheses are therefore not supported.

Interpretation

A total of 28 hypotheses were tested in this dissertation. Of the 28 hypotheses tested, evidence was found to support 11 and the overall findings were quite good. Three primary forms of analyses were performed; a group difference analysis which tested 3 hypotheses, a prediction analysis which tested 20 hypotheses, and a moderation analysis which tested 5 hypotheses. The 3 group difference hypotheses and the 5 moderation hypotheses were not supported. Of the 20 prediction hypotheses, all but 9 were supported. The 20 prediction hypotheses included 10 hypotheses predicting relationships between the 4 new experience constructs. These new constructs had not been measured and the predictive relationships had not been previously tested. Of the 11 prediction hypotheses supported, 5 of the hypotheses involved the new experience constructs; therefore, this study was definitely successful. The interpretation of the findings of the hypotheses tests will now be presented, beginning with Hypotheses 1a through 10, summarized in Table 32.

Table 32 Hypotheses Tests 1a-10 Results

	Hypothesized Relationship	Standardized Estimate	S=Supported NS=Not Supported
H1a	Threat Severity will *positively* influence Behavioral Intent	.220***	S
H1b	Threat Severity will *negatively* influence Response Efficacy	.331***	S (-)
H1c	Threat Severity will *negatively* influence Self-efficacy	.037	NS
H2a	Threat Susceptibility will *positively* influence Behavioral Intent	.043	NS
H2b	Threat Susceptibility will *negatively* influence Response Efficacy	-.164*	S
H2c	Threat Susceptibility will *negatively* influence Self-efficacy	-.049	NS
H3	Response Efficacy will *positively* influence Behavioral Intent	.052	NS
H4	Self-efficacy will *positively* influence Behavioral Intent	.405***	S
H5	Response Cost will *negatively* Influence Behavioral Intent	-.254***	S
H6a	Direct Response Experience will *positively* influence Response Efficacy	.125	NS
H6b	Direct Response Experience will *positively* influence Self-efficacy	.899***	S
H6c	Direct Response Experience will *negatively* influence Response Cost	-.224*	S
H7a	Vicarious Response Experience will *positively* influence Self-efficacy	-.016	NS
H7b	Vicarious Response Experience will *positively* influence Response Efficacy	.288**	S
H7c	Vicarious Response Experience will *negatively* influence Response Cost.	.108	NS
H8a	Direct Threat Experience will *positively* influence Threat Severity	.018	NS
H8b	Direct Threat Experience will *positively* influence Threat Susceptibility	.177*	S
H9a	Vicarious Threat Experience will *positively* influence Threat Severity	.267***	S
H9b	Vicarious Threat Experience will *positively* influence Threat Susceptibility	.125	NS
H10	Social Influence will *positively* influence Behavioral Intent	.141*	S

*Significant at the p<.05 level
**Significant at the p<.01 level
***Significant at the p<.001 level

The first hypotheses developed in this study were those commonly found in studies where PMT is a foundational theory. Hypotheses 1a, 2a, 3, 4, and 5 were the most commonly tested predictive relationships between the PMT independent variables

of threat severity, threat susceptibility, response efficacy, self-efficacy, and response cost and the dependent variable behavioral intent. Hypothesis 1a and Hypothesis 4 predicted positive relationships between threat severity and behavioral intent and between self-efficacy and behavioral intent, respectively. Both of these hypotheses were strongly supported, representing evidence that an individual's perception of the severity of a threat and their self-efficacy to respond to the threat play a strong part in their intent to perform secure behaviors. These findings also lend additional strength to the findings of previous works where threat severity was found to strongly influence behavioral intent (Banks et al., 2010; Crossler, 2010; Garung et al., 2009; Malimage & Warkentin, 2010; Pahnila et al., 2007) and to those where self-efficacy was found to be a strong predictor of behavioral intent (Crossler, 2010; Garung et al., 2009; Ifinedo, 2012; Johnston & Warkentin, 2010; LaRose et al., 2008; Malimage & Warkentin, 2010; Woon et al., 2005; Zhang & McDowell, 2009).

Hypothesis 5 predicted a negative relationship between response cost and behavioral intent. Strong evidence was found to support the hypothesis, adding to the belief that when the costs of performing a response are perceived by an individual to be too high, there is a likelihood that the individual will choose not to perform the secure behavior. This particular predicted relationship is one that has produced mixed findings from one context to another, having had previous studies find response cost to be both an important explanatory variable (Herath & Rao, 2009; Lee & Larsen, 2009; Zhang & McDowell, 2009) as well as an insignificant predictor (Crossler, 2010; Garung et al., 2009) of individual attitudes and behaviors.

Hypothesis 2a which predicted a positive relationship between threat susceptibility and behavioral intent and Hypothesis 3 which predicted a positive

relationship between response efficacy and behavioral intent, however, were not supported. Mixed findings have been reported for the predicted relationship between threat susceptibility and behavioral intent in past studies. This dissertation adds support to those studies that reported threat susceptibility was an insignificant predictor of behavioral intent (Malimage & Warkentin, 2010) but contrary to the findings of those reporting a significant relationship (Ifinedo, 2012; Ng et al., 2009; Pahnila et al., 2007; Woon et al., 2005). The findings reported here are also contrary to those reported for the relationship between response efficacy and behavioral intent where a large number have found the relationship to be significant (Crossler, 2010; Garung et al., 2009; Ifinedo, 2012; LaRose et al., 2008; Malimage & Warkentin, 2010; Zhang & McDowell, 2009).

As discussed in the literature review of this dissertation, the relationships between the threat assessment and the coping assessment variables are frequently tested in earlier PMT studies (Floyd et al, 2000; Milne et al., 2000), but has rarely been tested in PMT studies to date. Hypotheses 1b, 1c, 2b, and 2c test the relationships among the PMT independent variables. As found in a previous PMT study conducted in the context of IS security (Johnston & Warkentin, 2010), the tests of these relationships produced support for negative relationships between threat severity and response efficacy and between threat severity and self-efficacy. While negative relationships were also predicted between threat susceptibility and response efficacy and between threat susceptibility and self-efficacy, the study did not find support for these two relationships. The findings of this dissertation agreed with the findings reported in the previous study in that support was found for the relationship between threat severity and response efficacy and no support was found for the relationship between threat susceptibility and self-efficacy; however, threat severity was found to be strongly related to response efficacy in a

positive rather than negative direction in this dissertation unlike the previous study where the negative relationship was supported. The findings in this dissertation study differed from the previous study further by finding support for the negative relationship between threat susceptibility and response efficacy, and by failing to find support for the negative relationship between threat severity and self-efficacy. The results of these two studies provide compelling evidence of the existence of relationships among the PMT independent variables, but the inconsistency of the findings between the studies requires additional tests to more clearly understand those relationships.

The Hypotheses 6a through 9b were the predictive relationships of the 4 new experience constructs with the PMT constructs. This dissertation is believed to be the first instance to date where the predictive relationships between these constructs were tested in this context. Hypotheses 6a through 6c, respectively, predicted that response efficacy and self-efficacy would be positively influenced and response cost would be negatively influenced by direct response experience. The statistical tests found no evidence to support Hypothesis 6a. This suggests that an individual's perception of the efficacy of a response may not be affected by the individual's direct experience with that response. However, the evidence found did support Hypotheses 6b and 6c in both direction and strength. The strength of the relationship predicted in Hypothesis 6b, which was between direct response experience and self-efficacy, was the strongest relationship in the model. The correlation was found to be .899 with a C.R of 15.053. This extremely strong relationship is not surprising, as these two constructs were found to load on the same factor during the EFA analyses. Additionally, the definitions of direct response experience and self-efficacy are similar, and experience is known to be strongly related to self-efficacy (Bandura, 1977; Gist & Mitchell, 1992). This result further establishes that

an individual's direct experience with a response is a strong positive predictor of his/her self-efficacy to perform the response. The findings to support Hypothesis 6c indicate that an individual's experience with a response will also positively predict his/her perception of the cost of performing the response.

Hypotheses 7a through 7c, respectively, predicted that self-efficacy and response efficacy would be positively influenced and response cost would be negatively influenced by vicarious response experience. The statistical tests found evidence to support Hypothesis 7b, but not Hypotheses 7a and 7c. This suggests that an individual's experience that was gained vicariously can affect the individual's perception of the efficacy of the response. The vicarious experience may not, however, affect his/her perception of self-efficacy to respond to the threat or his/her perception of the cost of performing the response.

Hypotheses 8a and 8b predict positive relationships between direct threat experience and both threat severity and threat susceptibility. Evidence was found to support Hypothesis 8b indicating that an individual's perception of susceptibility to a threat is influenced by direct experience with that threat. Hypothesis 8a was not supported which indicates that the perception of severity of a threat is not influenced by direct experience with the threat.

Hypotheses 9a and 9b predict positive relationships between vicarious threat experience and both threat severity and threat susceptibility. The results of the statistical tests found strong evidence to support Hypothesis 9a, but not Hypothesis 9b. This suggests that an individual's experience gained vicariously may not influence his/her perception of susceptibility to a threat, but that it may strongly influence his/her perception of severity of a threat.

Hypotheses 10 through 11e predicted direct and moderating influences of the Social Influence construct. While not traditionally included in PMT studies, Social Influence is quite frequently explored in behavioral IS research and has recently proven to perform well as a predictor of variance in IS security studies (Johnston & Warkentin, 2010; Lee & Larsen, 2009; Lu et al., 2005). Studies are more often being found to include this important explanatory variable, including this dissertation study. Hypothesis 10 was the last hypothesis tested in the prediction analysis and predicted that social influence would play a direct part in positively influencing behavioral intent. The statistical tests found evidence to support Hypothesis 10, indicating that the influence of others does play a part in the behavioral choices made by individuals regarding information security. This lends further support to previous studies that also found SOC influences behavioral intent (Anderson & Agarwal, 2010; Banks et al., 2010; Ifinedo, 2012; Johnston & Warkentin, 2010; Pahnila et al., 2007).

The literature reviewed conducted in this dissertation study did not find that the moderating effects of SOC are commonly tested in PMT studies within the context of IS security; nonetheless, Hypotheses 11a through 11e, summarized in Table 33, tested such relationships. These hypotheses predicted that SOC would moderate the relationships between the PMT variables of threat severity, threat susceptibility, response efficacy, and self-efficacy, and the DV behavioral intent. The statistical tests performed found no evidence that social influence had any influence on the strength or direction of any of the hypothesized relationships between threat severity, threat susceptibility, response efficacy, or self-efficacy and behavioral intent. Because no evidence to support these relationships was found, and because no previous research testing these relationships was evident, it may be that SOC has only a direct influence on behavioral intent.

Table 33 Results of Hypotheses Tests 11a-11e

	Hypotheses	S=Supported NS=Not Supported
H11a	A higher Social Influence will result in Self-efficacy having a stronger *positive* influence on Behavioral Intent	NS
	A lower Social Influence will result in Self-efficacy having a weaker *positive* influence on Behavioral Intent	NS
H11b	A higher Social Influence will result in Threat Susceptibility having a stronger *positive* influence on Behavioral Intent	NS
	A lower Social Influence will result in Threat Susceptibility having a weaker *positive* influence on Behavioral Intent	NS
H11c	A higher Social Influence will result in Response Cost having a stronger *negative* influence on Behavioral Intent	NS
	A lower Social Influence will result in Response Cost having a weaker *negative* influence on Behavioral Intent	NS
H11d	A higher Social Influence will result in Threat Severity having a stronger *positive* influence on Behavioral Intent	NS
	A lower Social Influence will result in Threat Severity having a weaker *positive* influence on Behavioral Intent	NS
H11e	A higher Social Influence will result in Response Efficacy having a stronger *positive* influence on Behavioral Intent	NS
	A lower Social Influence will result in Response Efficacy having a weaker *positive* influence on Behavioral Intent	NS

The tests of Hypotheses 12 through 14 were operationalized through the use of an experimental component. The data collection method used was the Solomon Four Group Design modified to include six groups so as to accommodate two treatments. The two treatments tested were 1) the persuasive message of a fear appeal which served as the proxy for awareness instruction, and 2) the persuasive fear appeal message accompanied by additional instructions regarding recommended responses to the threat which served as the proxy for training instruction. In order to gauge the effectiveness of the treatments on the participants' behavioral intent toward performing a recommended secure behavior over the behavioral intent of those participants' exposed to no treatment, a series of

ANOVA and t-tests were performed on the groups. As shown in Table 34, no differences were found among the groups indicating a lack of support for Hypotheses 12, 13, and 14.

Table 34 Results of Hypotheses Tests 12-14

	Hypotheses	S=Supported NS=Not Supported
H12	Individuals who are exposed to a fear appeal regarding an ISP threat and response will show higher intent to perform the recommended secure behavior than individuals who are not exposed to the fear appeal.	NS
H13	Individuals who are exposed to a fear appeal and response training will show higher intent to perform the recommended secure behavior than individuals who are not exposed to the fear appeal and response training.	NS
H14	Individuals who are exposed to a fear appeal and response training will show higher intent to perform the recommended secure behavior over that of individuals who are exposed to a fear appeal alone.	NS

Post Hoc Analysis

The statistical technique of SEM is a confirmatory technique and as such, the decision to re-specify a model post hoc is equivalent to moving from a confirmatory to an exploratory phase of the analysis (Byrne, 2010; Hair et al., 2010; Tabachnick & Fidell, 2007). A post hoc analysis should be performed only if there is evidence to support it and most importantly if it is justified by theory. Additionally, a post hoc analysis may be performed to test alternative models in order to further support the research model and lend strength to the statistical findings, or to develop a more parsimonious model. While no strong evidence was found indicating the need to re-specify the model and no compelling theoretical justification to re-specify the model was evident, this study is fundamentally an exploratory study because it is the first time to test the new experience constructs which expand the PMT model. Therefore, a post hoc analysis was conducted

to more fully explore and to gather complete statistical evidence to support the proposed model in this study.

The statistical findings indicated several paths in the model were insignificant and as such, were not making a useful contribution to the explanatory power of the model. An alternate model was developed through the iterative removal of the insignificant paths in the original model. The least significant path was between direct threat experience and threat severity. The path was removed and the model fit statistics and path estimates were examined and compared to the original model to determine if there had been any improvement. The model fit statistics remained the same, and the path between vicarious threat experience to threat severity which had been significant in the original model remained significant and the estimate improved slightly from .267 to .278. All other path estimates were unchanged from the original model.

The next least significant path identified in the model was between vicarious response experience and self-efficacy. After its removal, the Chi-square Index showed minor improvement changing from 1.80 to 1.79, but the remaining model fit statistics were unchanged. The path estimate between direct response experience and self-efficacy remained significant but decreased from .899 to .888. All other path estimates remained unchanged. The trimming of insignificant paths continued through a total of nine iterations until all paths remaining were statistically significant. This model trimming process resulted in a more parsimonious model with better model fit. Table 35 lists the final model fit statistics as compared to the proposed model and Table 36 lists the path relationships remaining in the final re-specified model with the standardized estimates and the level of significance as compared to the proposed model.

Table 35 Structural Model Fit Statistics Comparison

Statistic	Recommended Value	Proposed Model	Re-specified Model
Chi-square Statistic	--	781.885	791.167
Degrees of freedom (df)	--	434	443
Chi-square Statistic significance	--	.000	.000
Chi-square Index (Chi-square/df)	<3	1.802	1.786
Root Mean Squared Residual (RMR)	≤.08	.076	.077
Goodness of Fit (GFI)	>.90	.869	.867
Adjusted Goodness of Fit (AGFI)	>.90	.840	.842
Normed Fit Index (NFI)	>.90	.899	.898
Comparative Fit Index (CFI)	>.90	.952	.952
Root Mean Square Error of Approximation (RMSEA)	≤.08 / ≤.06	.051	.051

Table 36 Structural Model Parameter Estimates Comparison

	Original Model		Re-specified Model	
Relationship	Standardized Estimate	p	Standardized Estimate	p
TSV→BEH	.220	***	.245	***
TSV→REF	.331	***	.337	***
TSU→REF	-.164	.012*	-.158	.014*
SEF→BEH	.405	***	.424	***
RSC→BEH	-.254	***	-.248	***
DRE→SEF	.899	***	.889	***
DRE→RSC	-.224	.012*	-.154	.014*
VRE→REF	.288	.001**	.378	***
DTE→TSU	.177	.026*	.243	***
VTE→TSV	.267	***	.279	***
SOC→BEH	.141	.008*	.148	.005**

*Significant at the p<.05 level
**Significant at the p<.01 level
***Significant at the p<.001 level

Interpretation

The re-specified model fit statistics, shown in Table 35, show the Chi-square Index decreased from 1.802 to 1.786, and the RMR and AGFI levels increased from .076

to .077 and from .840 to .842, respectively. Overall, the model re-specification resulted in an improved model fit.

The re-specified model, shown in Figure 11 with the final standardized estimates and SMC values noted, includes only the significant paths which represent the eleven supported hypotheses. All of the significant paths in the proposed model either remained at the same level of significance or improved to greater significance, and most of the path estimates increased indicating a stronger predictive model. One path in particular, path between vicarious response experience to response efficacy, saw an increase in the estimate from .288 at the $p<.01$ level of significance to .378 at the $p<.001$ level of significance.

The notable construct SMC values were again those of self-efficacy, behavioral intent, and response efficacy. The SMC for behavioral intent, which was about the same as for the proposed model, indicated that the model explained 42.7% of the variance in behavioral intent. The SMC for self-efficacy was also about the same as in the proposed model, but the SMC for response efficacy increased from .298 to .312.

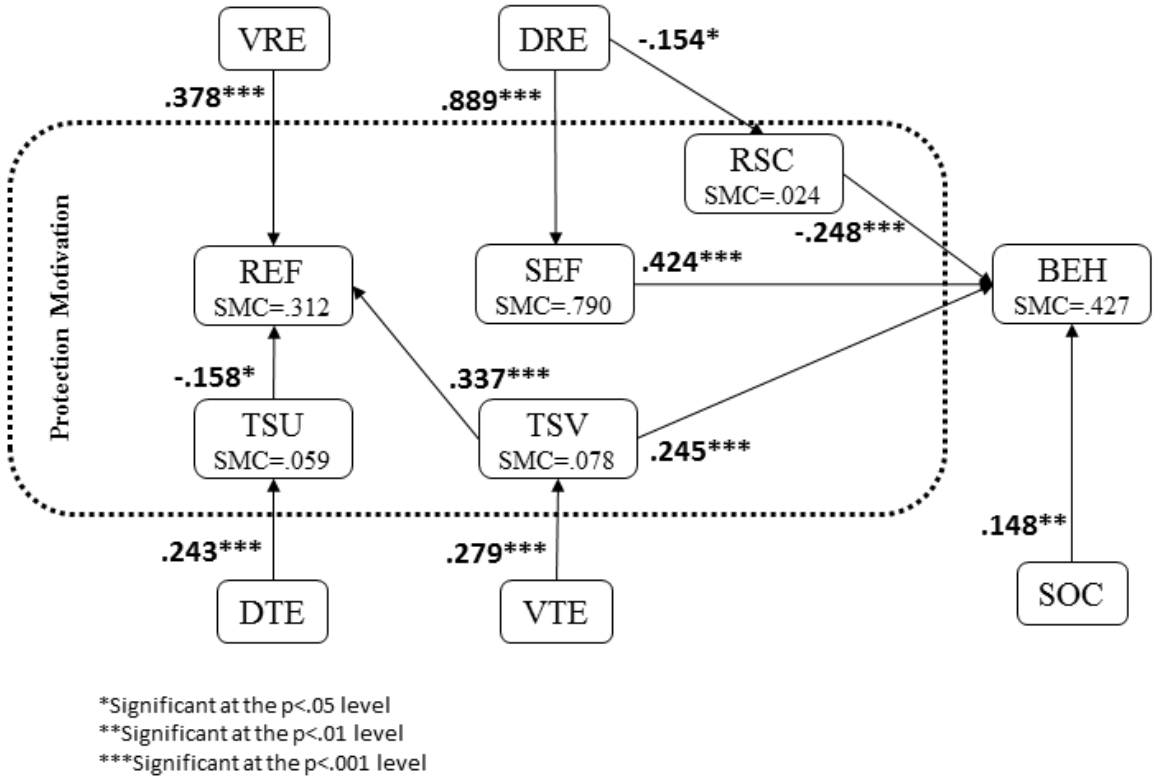

Figure 11 Re-specified Structural Model with Standardized Estimates

Summary

The results of the statistical analyses performed in this dissertation were presented in this chapter. A pilot study was performed first, and the analyses which focused on EFA were described and the findings were presented. The primary study was performed next, and included an EFA analysis, analyses of group comparisons, followed by SEM analyses of the measurement and structural models proposed in this study, and finally, tests for moderation effects were described and the findings presented. Evidence of validity and reliability was presented, and the proposed models were found to have acceptable fit with the data in this study. Out of the 28 hypotheses proposed and tested, evidence was found to support 11 of them, with the 4 new experience constructs developed in this dissertation accounting for 5 of the supported hypotheses. A post hoc

analysis was performed and the resulting model included support for the same hypotheses but was more parsimonious, had better fit to the data, and overall exhibited greater explanatory power.

CHAPTER V

CONCLUSION

The purpose of this dissertation was to answer three research questions. The first question was "What role does an individual's past experience with an information security threat play in the individual's ISP compliance behavioral intent?" and proposed to explore the relationship between an individual's past experience, both direct and vicarious, with information security *threats* and his/her intent to behave in a secure manner. The secure manner in which we desire for individuals to behave, in general, is known as a secure response. Therefore, the second question was "What role does an individual's past experience with performing an information security response play in the individual's ISP compliance behavioral intent?" and proposed to explore the relationship between an individual's past experience, again both direct and vicarious, with the *responses* to information security threats and his/her intent to behave in a secure manner. The third question was "Will use of response training with a fear appeal more likely result in individuals acting in a secure manner than with use of a fear appeal alone?" This question introduced theory and practice into the study by comparing two forms of secure behavior encouragement; the use of a fear appeal as compared to the use of a fear appeal accompanied by information security response instruction. Through the attempt to answer these questions, 28 hypotheses were developed and the expansion of the established theory of PMT was tested. This study produced evidence to indicate that experience does indeed play an important role in an individual's behavioral choices

towards information security, and as such the first two research questions were provided with initial answers and the support for further study. This study produced results that appear to indicate that the answer to the third research question is that there is no benefit toward influencing individual behavior from using response training with a fear appeal over that of a fear appeal alone. However, because no influence by the fear appeal alone was found either, the true answer to the question is not known as supported by this dissertation research, and further study is required.

Study Summarization

The research method that was followed included two separate phases of data collections with data analyses. The first data collection phase was primarily focused on refinement of the measures and refinement of the experimental method. A series of expert panels were conducted to gain the input and advice from experts in instrument development and data collection in general and in information security in particular. The measures used and the instrument were revised prior to conducting a pilot study. The instrument was web-based and hosted through the online survey host Qualtrics. A small convenience population of 65 students enrolled in classes at the MSU College of Business during the 2012 Maymester session fully participated in the pilot study. The pilot data was analyzed with an EFA and the initial discriminant and convergent validities and internal reliabilities of the measurement scales were assessed. The overall results of the pilot study suggested that the instrument and measures were adequate and ready to be tested in the primary study phase.

The second data collection phase was the primary study, again conducted in an online environment at a site hosted by Qualtrics. The population included students,

faculty, and staff at MSU. The snowball data collection method was used to expand the participation invitation beyond the boundaries of MSU to include friends, relatives, and co-workers of the students, faculty, and staff of MSU. Additional participation invitations were distributed through a Facebook post and by sending an invitation on two separate occasions to the members of the Association for Information Systems through the membership listserv. A total of 633 individuals accessed the online instrument, and the usable data set included 311 cases.

This dissertation study included an experimental component and the Solomon Four Group Design was used to collect data in the primary study. Through the random assignment of individuals to one of four possible groups exposed to all combinations of the pretest, treatment, and posttest, this method allows for the control of internal and external validity threats. Because two treatments were tested in this study, the Solomon Four Group Design was modified to include six groups and thereby accommodate the data collection for those individuals exposed to the second treatment.

The data analyses included tests of the internal and external validity of the experimental component, verification of the validity and reliability of the measures, and hypotheses tests. A series of t-tests and ANOVA tests were conducted to test for internal and external validity of the experiment. The tests found evidence of external validity of the experimental method which indicated that the pretest did not influence the treatments. The internal validity tests, however, found no differences in the DV of the pretest or posttest between or among the groups. This indicated that neither of the treatments was effective in influencing the respondents' behavioral intent.

With the results of the data analyses showing that the data groups did not differ from one another, the groups of data could be combined to create a larger data for the

remaining analyses. The raw data was revisited and cleaned removing all but the cases with complete pretest responses, resulting in a total of 306 cases available for analysis. The respondents in the majority (94%) of the 306 cases had answered "yes" when asked the filter question "Do you regularly use a computer that also stores personal, sensitive, or valuable information that you want protected?" indicating strong support that the population was appropriate for this dissertation study.

An EFA was conducted on the primary study data set. One item measure, VRE2, was determined to be a poor measure and was removed to improve the model. Only 10 factors rather than 11 factors emerged from the data, with the self-efficacy and direct response experience item measures loading strongly together on one factor. All other indicators of convergent and discriminant validity of the measures were present, and the internal reliability tests were quite good as well. Therefore, the decision was made to retain both self-efficacy and direct response experience in the study and to proceed with the understanding that the two constructs were highly correlated.

A confirmatory analysis was conducted next using a two-step approach (Anderson & Gerbing, 1988) which used the technique of SEM. The approach began with a test of the measurement model to establish evidence of validity and reliability, followed by a test of the structural model to establish evidence of predictive validity. The results of both of the models indicated that while there was room for improvement, as is the case for all research studies (McGrath, 1995), overall the model was deemed acceptable.

The final analysis conducted included tests for moderating affects by SOC on threat severity, threat susceptibility, response efficacy, and self-efficacy and each of the construct's relationship with behavioral intent. Two methods were used; group analysis

and interaction analysis, and both methods produced findings indicating there was no evidence of moderation present in the model with the primary data set.

There were 28 hypotheses tested in this dissertation study. Evidence was found to support a total of 11. The hypotheses predicting effectiveness of the experimental component were not supported. The hypotheses predicting moderating effects of SOC were not supported. The remaining hypotheses predicted relationships among the constructs in the study. About half of these last hypotheses were supported, 5 of which involved the new experience constructs, direct threat experience, vicarious threat experience, direct response experience, and vicarious response experience. The strong performance by the experience constructs in this study lent support to a strong start at answering the first two research questions in this dissertation study. Specifically, both direct experience and vicarious experience do play an important part in an individual's intention to behave in a secure manner regarding information security threats, and the results of this dissertation strongly support further study. The post hoc analysis performed reinforced the findings of the analyses conducted on the proposed model and successfully produced a more parsimonious model that better fit the data.

Implications

The goal of research is to make a contribution to both academia and to practice (Benbasat & Zmud, 1999; Lyytinen, 1999). The purpose of this dissertation was to explore the role of an individual's experience in the context of information security behavior. A well-established theory, PMT, provided the theoretical foundation. The study was conducted in a rigorous manner and followed proven methods of data collection and analyses. The Security Education, Training, and Awareness (SETA)

programs typically used by organizations within the United States to provide employees with instruction regarding information security provided the practical foundation. The study was designed such that a contribution would be made to both academia and to practice, regardless of the specific outcomes.

The primary contribution to academia proposed in this study was to expand the theory of PMT by including direct and vicarious experience regarding both threats and responses to the threats. The results of this study found that all four experience constructs do make an important contribution toward an individual's threat assessment, coping assessment, and therefore toward intent to perform secure behaviors. As clearly illustrated in the re-specified model shown in Figure 11, a distinct contribution to the PMT model is made by each of the four experience constructs. Specifically, an individual's experience with a threat was found to be a strong influence on his or her threat appraisal and an individual's experience with a response strongly influences his or her coping appraisal. Through the inclusion of both direct and vicarious experience, this research has provided evidence which supports the importance of both forms of experience as originally proposed by PMT. Specifically, this study revealed that within the context of IS security, direct experience affects the perception of threat susceptibility, but vicarious experience affects the perception of threat severity. Additionally, direct experience affects the perception of self-efficacy, but vicarious experience affects the perception of response efficacy. This implies that fear appeal effectiveness may be increased when knowledge of the levels and types of experience possessed by an individual are known and incorporated into the development of the fear appeal. A lack of knowledge regarding experience levels may partially explain why mixed results have been commonly reported in PMT studies in the field of IS security. Furthermore, this

also implies that the lack of knowledge of the respondents' experience was a likely contributor to the lack of desired results in the experimental component of this dissertation study.

The expansion of PMT may improve the theory's usefulness and add to its explanatory power within the context of information security research. Although both direct experience and vicarious experience are included in the original PMT research model, no PMT-based research was found that incorporates them both. Some form of experience construct is included in the majority of empirical IS research, but the definition, if one is included, has been found to vary widely, and the treatment and measurement are frequently inconsistent (Aguirre-Urreta & Marakas, 2008). This dissertation research provided clear, specific, and distinct definitions of all four forms of experience. With few exceptions (Shropshire, Warkentin, & Johnston, 2010; Warkentin et al., 2011), the measure of experience is typically operationalized as a single indicator to measure quantity or frequency (Constant et al., 1996; Sitren & Applegate, 2007). This dissertation developed valid and reliable unidimensional reflective measures for the four experience constructs, contributing scales to measure a richer experience construct than is commonly found in the extant literature.

Based on the literature review findings, the constructs that were predicted to have a direct influence on behavioral intent included response efficacy, threat severity, response cost, threat susceptibility, self-efficacy, and social influence. The evidence found in this study supported only response cost, self-efficacy, threat severity, and social influence as predictors of behavioral intent. No evidence was found to support either threat susceptibility or response efficacy as an influence on behavioral intent in this context. A closer examination of the re-specified model in Figure 11 reveals that while

the predictions of threat susceptibility and threat severity as influences on response efficacy held, the relationship between threat severity and response efficacy was predicted to be negative but was found to be very strongly positive. Furthermore, these three constructs, although strongly related, produced no direct impact on behavioral intent. These findings further support the value of exploring the interaction relationships that are typically neglected in fear appeal research performed in the field of IS but are included in research conducted in other fields. One implication that can be drawn from this evidence is that there may be an overall effect of a fear appeal on behavioral intent that is not evident from analyzing the individual relationships between the PMT constructs and behavioral intent. The fear appeal is a persuasive message and as such may actually represent a formative construct; therefore in order to measure the effect of the fear appeal on behavioral intent, the overall analysis of the relationship must be changed from that of reflective to formative.

Another interesting finding in this study includes the relationships between direct response experience, self-efficacy, response cost, and behavioral intent. Direct response experience was found to negatively impact an individual's perception of response cost, which in turn was negatively related to behavioral intent. Direct response experience also proved to be an extremely strong predictor of self-efficacy, a revealing and yet not surprising finding, as it is well known that a positive relationship between self-efficacy and an individual's level of experience exists (Bandura, 1977; Gist & Mitchell, 1992). While not specifically tested in this study, the implication from the findings of the tested predictions is that direct response experience is a positive predictor of behavioral intent. The evidence from this study implies that further research to test and better understand these relationships is important.

Another primary contribution to academia by this study was the test of previously validated existing measures and the test of relationships found to be significant in previous PMT-related studies. It is through replications in studies such as this dissertation that all research builds upon the works that have come before, and adds to the validity, reliability, and generalizability of the findings and of theories. The existing scales tested in this study successfully added to their validity and reliability. Several of the relationships tested that had been previously identified were upheld and therefore added support to them as well. Specifically, three of the five relationships between the PMT variables and behavioral intent, the paths from threat severity, self-efficacy, and response cost, were found to be very strong in this dissertation study. For example, the path estimate between self-efficacy and behavioral intent was .405 with a C.R. value of 7.327. Although the remaining two paths, threat susceptibility and response efficacy to behavioral intent, were not found to be significant, such findings are consistent with previous studies and implies that the explanatory power of PMT is dependent upon the context in which it is applied.

In summary, this dissertation research made several contributions to the existing body of knowledge that supports the usefulness of the theory of PMT in aiding to understand individual behaviors in the context of information security. Specifically, this dissertation presented strong evidence that experience does indeed play a role in the PMT model; therefore, an expansion of the PMT model to include the experience constructs of direct response experience, vicarious response experience, direct threat experience, and vicarious threat experience is justified.

The contribution to practice proposed was to incorporate a fear appeal into ISP instructional methods such as those used in SETA programs, with the intent to aid in

improving the programs to increase individual compliance with ISP. The experimental component was not successful in answering the research question proposed, and the contribution to practice became instead the strong performance of the experience constructs which demonstrated that all forms of experience, both direct and vicarious, and with the threats and with the responses, are important influences on individuals' behavioral choices regarding information security and should not be underestimated but should continue to be explored. Specifically, the findings of this study imply that to convey to employees the susceptibility of threats and the recommended use of secure responses, instructional programs should focus on hands-on instruction. However, to convey to employees the severity of threats and the effectiveness of the recommended responses, the traditional classroom-style instruction may suffice without the need for additional hands-on instruction.

Several additional questions became evident through this study. For example, because no difference was found between the treatments, the question of "Why was there no difference" is raised. As previously stated, a lack of knowledge regarding the level of experience possessed by the respondents may have contributed to the lack of effectiveness of the treatments. Or, it may be that taking a step back is required and we must first ask the question "Is a fear appeal a useful persuasive tactic to encourage individuals to behave in a secure manner?" before we attempt to repeat the comparison such as that made in this study. Another potential cause may be that the SETA programs as exemplified in this study are no longer effective. It may that a reassessment of individuals' perceptions of technology in general and information security in particular needs to be performed, because individuals are much more "tech savvy" than they were when the SETA programs were first designed and implemented in the 1990's. The NIST

guidelines on information security training requirements are being revised and are still in draft form as of fall of 2012, which is a strong indicator to support that the instructional programs themselves are due for a change. Regardless of the outcome of this dissertation study, the underlying question is still valid; "How can we improve individual compliance with ISP?" and therefore, continued research in this area is necessary as a contribution to practice.

Limitations

All research will contain flaws; therefore, care and thoroughness of planning, execution, and presentation are necessary to minimize the impact of those flaws (McGrath, 1995). This study is no exception and, while care was taken to reduce their impact, limitations exist and will now be discussed. The first limitation was that it did not model all of the real world attributes possible within the context. The more realistic a model is, the more complicated it will be to model and to analyze. A parsimonious model was selected for use, and in doing so the research study was limited. However, parsimony is a necessary objective in research that enables a researcher to focus on a smaller portion of a phenomenon and achieve results with greater clarity than would be possible otherwise.

The convenience sample used in this study was representative of another limitation. Because the respondents self-selected their participation in this study, they were not a true random sampling from the intended population. Therefore the sample includes biases which are unknown and cannot be measured (AAPOR, 2012). Additionally, the students, faculty, and staff of MSU are diverse in many respects, they are primarily from Mississippi and the states nearby and thus represent a narrow portion

of the true target population that encompasses all computer users in the United States who value and want to protect data. Additionally, the demographic characteristics captured indicated that the sample included a high percentage of well-educated individuals which introduced an additional bias. However, the contributions achieved through this exploratory study with this sample are valuable nonetheless, and represent an important first step in this specific area of study and also represent a contribution to information security research in general.

The size of the sample was appropriate for the statistical analyses conducted in this study and the results found are meaningful; however, the size limited the choices of analyses techniques available for use. A sample size in the 500-600 range would have enabled the data set to be split in order to conduct an EFA with one half and a CFA with the remaining half. This would have added strength to the findings regarding validity and reliability (MacKenzie et al., 2011). Also, if the sample size had been ≥ to 1,600, the ADF estimation method could have been used in the SEM analyses which would have added strength to the interpretations of the analyses (Byrne, 2010).

In hindsight, there are several possible reasons for the experimental component's lack of internal validity which limited this study. The literature review conducted found evidence that SETA programs fail more often than not; therefore, it is not particularly surprising that no difference was found between the awareness and the training instructional levels. The method of delivery or the focus on only one threat and one response may have also contributed to this issue. The experimental component must be redeveloped prior to any future test to prevent reoccurrence of this limitation.

The four new experience construct measures were tested for the first time in this study. The strength of the validity and reliability of a measure is dependent upon

repeated tests of the measures and the results achieved through those tests. Therefore, because this is the first study to test these new measures, the new measures limited the study; however, this is a limitation that is also a great strength, as it provides the foundation for future research to continue to explore these experience constructs.

Future Research

Important contributions to both academia and to practice were established by the completion of the study, and this dissertation provides an important beginning point for several additional research projects. For example, the limitations of this study that were identified in the previous paragraphs represent weaknesses that can be overcome through future research. The strengths of a study should also be used to identify future research because all research has room for improvement and expansion to other venues. It is with this mindset that potential future research directions are presented in the following final paragraphs of this dissertation.

This dissertation study should be refined and replicated with other samples, particularly samples from industry. Sampling from industry may affect the final data set size. For example, a centralized IT governance structure is often found in industry which can result in ISP compliance being perceived as more relevant than in academia where a decentralized IT governance structure is more common. The number of respondents participating may also be increased if other invitation methods are used.

The experiment should be refined prior to any plans for replication. Other delivery methods and forms of media should be considered and may be necessary to achieve successful treatment results. For example, rather than the text-based media found in this study, exploration into using verbal media, visual media, or a combination of

media should be conducted. Rather than an online delivery method, a face-to-face setting may be more successful and should be considered. Future studies could explore both varying types of media and delivery methods for the treatments.

The four new experience constructs performed well as latent variable measures in the context of this study, particularly given that they were newly developed and tested for the first time in this study. Latent construct measures should be tested multiple times and in varying contexts to increase their validity, reliability, and generalizability. A necessary future research direction will be to continue the development and test of the experience construct measures.

The direction of the relationships between experience and other constructs poses an additional area for future study. An individual's experience with a threat or with a response may be considered to be a positive experience or a negative experience in itself. Examples were found in the literature where experience played the role of a positive control variable (Pavlou & Gefen, 2004), or as a measure of a positive outcome (Sitren & Applegate, 2007). The present study did not attempt to explore the added characteristic of a positive or negative nature of the experience construct, yet past studies indicate it to be worth exploring.

Both direct and vicarious experience contributed to the predictive capabilities of the model and therefore two future research questions could be explored. "Which plays a stronger role in an individual's ISP compliance behavioral intent – direct or vicarious experience with an information security threat?" and "Which plays a stronger role in an individual's ISP compliance behavioral intent – direct or vicarious experience with an information security response?"

Last, the relationship between direct response experience and self-efficacy must be more closely examined through the performance of future research. The highly established construct of self-efficacy is so important in behavioral research in general and in IS research in particular that this relationship demands more in-depth research to achieve better understanding. The results of the EFA led to a proposal in this study that a multi-dimensional construct exists and direct response experience and self-efficacy are two of the dimensions. The results of the CFA support the belief that direct response experience may be a significant antecedent of self-efficacy, a relationship well-established in the self-efficacy literature (Bandura, 1977). Therefore, future studies will be performed to focus on understanding and explaining the direct response experience to self-efficacy relationship.

REFERENCES

AAPOR. (2012). Opt-in surveys and margin of error. Retrieved October 27, 2012, from http://aapor.org/Opt_In_Surveys_and_Margin_of_Error1/4195.htm

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24*(4), 665-694.

Aguirre-Urreta, M. I., & Marakas, G. M. (2008). *When more isn't necessarily better: Conceptualization and use of the experience construct in IS research.* Paper presented at the 39th Annual Meeting of the Decision Sciences Institute, Baltimore, MD.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Springer Series in Social Psychology* (pp. 11-39). Berlin: Springer.

Algie, J., & Rossiter, J. R. (2010). Fear patterns: A new approach to designing road safety advertisements. *Journal of Prevention & Intervention in the Community, 38*(4), 264-279.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavior intentions. *MIS Quarterly, 34*(3), 613-643.

Anderson, E. E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security, 27*(1/2), 22-29.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

Ariss, S. S. (2002). Computer monitoring: Benefits and pitfalls facing management. *Information & Management, 39*, 553-558.

Ballard, L., Lopresti, D., & Monrose, F. (2007). Forgery quality and its implications for behavioral biometric security. *IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, 37*(5), 1107-1118.

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

Banks, M. S., Onita, C. G., & Meservy, T. O. (2010). Risky Behavior in Online Social Media: Protection Motivation and Social Influence. *Americas Conference on Information Systems Proceedings*, Paper 372.

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173-1182.

Barrett, P. (2005). What if there were no Psychometrics? Constructs, complexity, and measurement. *Journal of Personality Assessment, 85*(2), 134-140.

Bassellier, G., Benbasat, I., & Reich, B. H. (2003). The influence of business managers' IT competence on championing IT. *Information Systems Research, 14*(4), 317-336.

Bearden, W. O., Hardesty, D. M., & Rose, R. L. (2001). Consumer self-confidence: Refinements in conceptualization and measurement. *Journal of Consumer Research, 28*(1), 121-134.

Benbasat, I., & Zmud, R. W. (1999). Empirical research in Information Systems: The practice of relevance. *MIS Quarterly, 23*(1), 3-16.

Bentler, P. M. (2005). *EQS 6 Structural Equations Program Manual*. Encino, CA: Multivariate Software.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin, 88*(3), 588-606.

Bishop, M. (2003). What is computer security? *IEEE Security & Privacy, 1*(1), 67-69.

Boncella, R. J. (2002). Wireless Security: An Overview. *Communications of AIS, 9*, 269-282.

Boss, S. R., Kirsch, L. J., Angermeier, I., & Boss, R. W. (2009). *Familiarity breeds content: How fear of cybercrime influences individual precaution-taking behavior*. Paper presented at the International Workshop on Informatin Systems Security Research.

Braver, M. C. W., & Braver, S. L. (1988). Statistical treatment of the Solomon Four-Group design: A meta-analytic approach. *Psychological Bulletin, 104*(1), 150-154.

Browne, M. W., & Cudeck, R. (1993). Alternative Ways of Assessing Model Fit. In K. A. Bollen & J. S. Long (Eds.), *Testing Structural Equation Models* (pp. 136-162). Newbury Park, CA: Sage.

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-A527.

Byrne, B. M. (1998). *Structural Equation Modeling with Lisrel, Prelis and Simplis: Basic Concepts, Applications and Programming* Mahwah, NJ: Lawrence Erlbaum Associates, Publishers.

Byrne, B. M. (2010). *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming* (2nd ed.). New York, NY: Routledge Taylor & Francis Group.

Campbell, D. T., & Stanley, J. C. (1963). Experimental and Quasi-experimental Design for Research *Experimental and Quasi-experimental Design for Research*. Boston, MA: Houghton Mifflin Company.

Carmines, E. G., & McIver, J. P. (1981). Analyzing Models with Unobserved Variables: Analysis of Covariance Structures. In G. W. Bohrnstedt & E. F. Borgatta (Eds.), *Social Measurement: Current Issues* (pp. 65-115). Beverly Hills, CA: Sage.

Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. *Information Systems Research, 20*(2), 198-217.

Chin, W. W., & Todd, P. A. (1995). On the use, usefulness, and ease of use of structural equation modeling in MIS research: A note of caution. *MIS Quarterly, 19*(2), 237-246.

Churchill, G. A. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. *Journal of Marketing Research, 16*, 64-73.

Churchill, G. A., & Peter, J. P. (1984). Research design effects on the reliability of rating scales: A meta-analysis. *Journal of Marketing Research, 21*, 360-375.

Chuvakin, A. (2010). Security Predictions 2020 (!). Blog Retrieved from http://chuvakin.blogspot.com/2010/01/security-predictions-2020.html

Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment, 7*(3), 309-319.

Constant, D., Sproull, L., & Kiesler, S. (1996). The kindness of strangers: The usefulness of electronic weak ties for technical advice. *Organization Science, 7*(2), 119-135.

Crossler, R. E. (2010). *Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data.* Paper presented at the 43rd Hawaii International Conference on System Sciences, Koloa, Kauai, Hawaii.

Crossler, R. E., & Belanger, F. (2009). The effects of security education training and awareness programs and individual characteristics on end user security tool usage. *Journal of Information System Security, 5*(3), 3-22.

Crossler, R. E., Johnston, A. C., Bélanger, F., & Warkentin, M. (2012). Theory adaptation for unstable IS phenomena: A punctuated equilibrium perspective. *Working Paper*.

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.

Davis, M. A. (2010). Global Threat, Local Pain: 2010 Strategic Security Survey *InformationWeek Analytics*: InformationWeek.

Davis, M. A. (2011). 2011 Strategic Security Survey: CEOs Take Notice *InformationWeek Analytics*: InformationWeek.

de Leeuw, E. D., Hox, J. J., & Dillman, D. A. (2008). *International Handbook of Survey Methodology*. New York, NY: Taylor & Francis Group.

DeVellis, R. F. (2003). Understanding the Latent Variable *Scale Development: Theory and Applications* (2nd ed., pp. 14-26). Thousand Oaks, CA: Sage Publications.

DeZabala, T., & Baich, R. (2010). Cyber crime: A clear and present danger *Center for Security & Privacy Solutions* Deloitte & Touche LLP.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Dillard, J. P., & Anderson, J. W. (2004). The Role of Fear in Persuasion. *Psychology & Marketing, 21*(11), 909-926.

Diversity Statistics - Campus Wide. (2011). Retrieved 1/27/2012, from http://odep.msstate.edu/pdfs/DiversityStatistics.pdf

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*(3), 201-209.

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18*(4), 21-39.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading, Massachusettes: Addison-Wesley Pub. Co.

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*, 408-420.

Forget, A., Chiasson, S., & Biddle, R. (2007). *Persuasion as Education for Computer Security.* Paper presented at the Association for the Advancement of Computing in Education (AACE) E-Learn.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservabe variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*, 352-357.

Garung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management & Computer Security, 17*(3), 276-289.

Garver, M. S., & Mentzer, J. T. (1999). Logistics research methods: Employing structural equation modeling to test for construct validity. *Journal of Business Logistics, 20*(1), 33-57.

Gaskin, J. (Producer). (2011a). Common Method Bias. Retrieved from http://www.youtube.com/watch?v=w7zZCBlRXog

Gaskin, J. (Producer). (2011b). Interaction Moderation (SEM). Retrieved from http://www.youtube.com/watch?v=K34sF_AmWio

Gaskin, J. (2012a). The Stats Tools Package. Retrieved from http://statwiki.kolobkreations.com/wiki/Main_Page

Gaskin, J. (2012b). Structural Equation Modeling (SEM): Interaction Retrieved September 9, 2012, from http://statwiki.kolobkreations.com

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega, 28*(6), 725-737.

Gerbing, D. W., & Anderson, J. C. (1988). An updated paradigm for scale development incorporating unidimensionality and its assessment. *Journal of Marketing Research, 25*(2), 186-192.

Gist, M. E., & Mitchell, T. R. (1992). Self-efficacy: A theoretical analysis of its determinants and malleability. *Academy of Management Review, 17*(2), 183-211.

Hair, J. F. J., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

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

Hu, L.-T., & Bentler, P. M. (1995). Evaluating Model Fit. In R. Hoyle (Ed.), *Structural Equation Modeling: Concepts, Issues and Applications* (pp. 76-99). Thousand Oaks, CA: Sage.

Hu, L.-t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55.

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.

Janis, I. L., & Feshbach, S. (1953). Effects of fear-arousing communications. *The Journal of Abnormal and Social Psychology, 48*(1), 78-92.

Janis, I. L., & Feshbach, S. (1954). Personality differences associated with responsiveness to fear-arousing communications. *Journal of Personality, 23*, 154-166.

Johnston, A. C., & Hale, R. O. N. (2009). Improved Security through Information Security Governance. *Communications of the ACM, 52*(1), 126-129.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549-A544.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kaplan, D. (2010). Weakest link: End-user education. *SC Magazine*. Retrieved from SC Magazine For IT Security Professionals website: http://www.scmagazineus.com/weakest-link-end-user-education/article/161685/

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), 518-555.

Kelloway, E. K. (1998). *Using LISREL for Structural Equation Modeling: A Researchers Guide*. Thousand Oaks, CA: SAGE Publications, Inc.

Kim, S., Cha, J., Knutson, B. J., & Beck, J. A. (2011). Development and testing of the Consumer Experience Index (CEI). *Managing Service Quality, 21*(2), 112-132.

Kirk, R. E. (2009). Experimental Design. In R. E. Millsap & A. Maydeu-Olivares (Eds.), *The SAGE Handbook of Quantitative Methods in Psychology*. Thousand Oaks, CA: SAGE Publications Inc.

Kline, K. N., & Mattson, M. (2000). Breast self-examination pamphlets: A content analysis grounded in fear appeal research. *Health Communication, 12*(1), 1-21.

Kline, R. B. (2011). *Principles and Practice of Structural Equation Modeling* (3rd ed.). New York, NY: The Guilford Press.

Kolb, N., & Abdullah, F. (2009). Developing an Information Security Awareness Program for a Non-Profit Organization. *International Management Review, 5*(2), 103-107.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM, 51*(3), 71-76.

LaRose, R., Rifon, N. J., Liu, S., & Lee, D. (2005). Understanding online safety behavior: A multivariate model *Comunication and Technology Division* International Communication Association.

Lee, G., Lee, J., & Sanford, C. (2010). The roles of self-concept clarity and psychological reactance in compliance with product and service recomendations. *Computers in Human Behavior, 26*, 1481-1487.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems, 50*, 361-369.

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

Levy, Y., & Ellis, T. J. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of Information, Knowledge, and Management, 6*, 151-161.

Lewis, B. R., Templeton, G. F., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems, 14*(3), 388-400.

Lewis, I. M., Watson, B., Tay, R., & White, K. M. (2007). The role of fear appeals in improving driver safety: A review of the effectiveness of fear-arousing (threat) appeals in road safety advertising. *International Journal of Behavioral and Consultation Therapy, 3*(2), 203-222.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Lindsey, L. L. M. (2005). Anticipated guilt as behavioral motivation: An examination of appeals to help unknown others through bone marrow donation. *Human Communication Research, 31*(4), 453-481.

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.

Loveland, G., & Lobel, M. (2010). Trial By Fire*Connected Thinking: What global executives expect of information security in the middle of the world's worst economic downturn in thirty years *Advisory Services*: PriceWaterhouseCoopers.

Lu, J., Yao, J. E., & Yu, C.-S. (2005). Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology. *Journal of Strategic Information Systems, 14*, 245-268.

Lyytinen, K. (1999). Empirical research in information systems: On the relevance of practice in thinking of IS research. *MIS Quarterly, 23*(1), 25-28.

MacKenzie, S. B. (2003). The dangers of poor construct conceptualization. *Journal of the Academy of Marketing Science, 31*(3), 323-326.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293-334.

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*, 469-479.

Malimage, K., & Warkentin, M. (2010). *Data loss from storage device failure: An empirical study of protection motivation.* Paper presented at the 2010 Workshop on Information Security and Privacy (WISP), St. Louis, MO.

Marett, K., McNab, A. L., & Harris, R. B. (2011). Social networking websites and posting personal information: An evaluation of Protection Motivation Theory. *AIS Transactions on Human-Computer Interaction, 3*(3), 170-188.

McGahee, T. W., & Tingen, M. S. (2009). The use of the Solomon Four-Group Design in nursing research. *Southern Online Journal of Nursing Research, 9*(1).

McGrath, J. E. (1995). Methodology matters: Doing research in the behavioral and social sciences. In R. M. Baecker, J. Grudin, W. A. S. Buxton & S. Greenberg (Eds.), *Human-computer Interaction: Toward the year 2000*. San Francisco, CA: Morgan Kaufmann Publishers Inc.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Mississippi State University Pocket FactBook. (Fall 2011). Retrieved from http://www.ir.msstate.edu/factbook_pocket11.pdf

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(2), 126-139.

Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures: Issues and applications*. Thousand Oaks, CA: Sage Publications, Inc.

Neuwirth, K., Dunwoody, S., & Griffin, R. J. (2000). Protection Motivation and Risk Communication. *Risk Analysis, 20*(5), 721-734.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the 40th Hawaii International Conference on System Sciences, Big Island, Hawaii.

Pallant, J. (2005). *SPSS Survival Manual: A Step by Step Guide to Data Analysis using SPSS* (2nd ed.). New South Wales, Australia: Allen & Unwin.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37-59.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security, 14*(2), 37-48.

Peter, J. P. (1979). Reliability: A review of Psychometric basics and recent marketing practices. *Journal of Marketing Research, 16*, 6-17.

Peterson, R. A. (1994). A meta-analysis of Cronbach's Coefficient Alpha. *Journal of Consumer Research, 21*, 381-391.

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in IS research. *MIS Quarterly, 31*(4), 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Prince, B. (2009). Survey Lists Top Enterprise Endpoint Security and Compliance Holes *eWeek*. Retrieved from eWeek Security Watch website: http://securitywatch.eweek.com/enterprise_security_strategy/survey_lists_top_endpoint_security_and_compliance_holes.html

Reuteman, R. (2011). Companies embrace telecommuting as a retention tool. Retrieved from CNBC.com website: http://www.cnbc.com/id/44612830

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

Richardson, R. (2011). 15th Annual 2010/2011 Computer Crime and Security Survey: Computer Security Institute.

Robinson, J. P., Shaver, P. R., & Wrightsman, L. S. (1991). Criteria for Scale Selection and Evaluation. In J. P. Robinson, P. R. Shaver & L. S. Wrightsman (Eds.), *Measures of Personality and Social Psychological Attitudes* (Vol. 1, pp. 1-15). San Diego, CA: Academic Press.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*, 93-114.

Roser, C., & Thompson, M. (1995). Fear appeals and the formation of active publics. *Journal of Communication, 45*(1), 103-121.

Sawilowsky, S., Kelley, D. L., Blair, R. C., & Markman, B. S. (1994). Meta-Analysis and the Solomon Four-Group Design. *The Journal of Experimental Education, 62*(4), 361-376.

Schwartz, M. J. (2010). Cyber threats forecast for 2011. *InformationWeek*. Retrieved from http://www.informationweek.com/news/security/reviews/227701135

Senior Scholars' Basket of Journals. (2011). (November 30, 2011). Retrieved from http://home.aisnet.org/displaycommon.cfm?an=1&subarticlenbr=346

Sherwood, A. L., & Covin, J. G. (2008). Knowledge acquisition in university-industry alliances: An empirical investigation from a learning theory perspective. *The Journal of Product Innovation Management, 25*, 162-179.

Shropshire, J. D., Warkentin, M., & Johnston, A. C. (2010). Impact of negative message framing on security adoption. *Journal of Computer Information Systems, 51*(1), 41-51.

Shuttleworth, M. (2009). Solomon Four Group Design. *Experiment Resources* Retrieved 1/18/2012, from http://www.experiment-resources.com/solomon-four-group-design.html

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M., Baskerville, R., & Heikka, J. (2006). A design theory for security information systems design methods. *Journal of the Association for Information Systems, 7*(11), 725-770.

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., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

Sitren, A. H., & Applegate, B. K. (2007). Testing the deterrent effects of personal and vicarious experience with punishment and punishment avoidance. *Deviant Behavior, 28*, 29-55.

Spitzner, L. (Producer). (2011, October 7, 2011). SANS Securing the Human. Retrieved from http://www.securingthehuman.org/resources

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security, 3*(2), 20.

Stafford, T. F., & Poston, R. (2010). Online security threats and computer user intentions. *Computer, 43*, 58-64.

Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly, 13*(2), 147-166.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision-making. *MIS Quarterly, 22*(4), 441-469.

Tabachnick, B. G., & Fidell, L. S. (2007). *Multivariate Statistics* (5th ed.). Boston, MA: Allyn and Bacon.

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly, 19*(4), 561-570.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security, 6*(4), 167.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective, 17*(5/6), 207-227.

Vance, A., Siponen, M., & Pahnila, S. (2009). *How personality and habit affect protection motivation*. Paper presented at the Association of Information Systems SIGSEC Workshop on Information Security & Privacy (WISP), Phoenix, AZ.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Vogt, W. P. (2005). *Dictionary of Statistics & Methodology: A Nontechnical Guide for the Social Sciences* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*, 191-198.

Warkentin, M., & Johnston, A. C. (2006). IT Security Governance and Centralized Security Controls. In M. Warkentin & R. Vaughn (Eds.), *Enterprise Information Assurance and System Security: Managerial and Technical Issues* (pp. 16-24). Hershey, PA: Idea Group Publishing.

Warkentin, M., & Johnston, A. C. (2008). IT Governance and Organizational Development for Security Management. In D. Straub, S. Goodman & R. L. Baskerville (Eds.), *Information Security Policies and Practices* (pp. 46-68). Armonk, NY: M.E. Sharpe.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267-284.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105.

Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. (SP800-16). Washington, D.C.: U.S. Government Printing Office.

Wilson, M., & Hash, J. (2003). *Building an information technology security awareness and training program*. (SP800-50). Washington, D.C.: U.S. Government Printing Office.

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

Witte, K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1*(4), 317-342.

Woon, I., Tan, G.-W., & Low, R. (2005). *A Protection Motivation Theory approach to home wireless security.* Paper presented at the International Conference on Information Systems.

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

Wright, R. T., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation, 19*(4), 391-416.

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems, 27*(1), 273-303.

Yount, R. (2006). *Research Design and Statistical Analysis in Christian Ministry* (4th ed.). Forth Worth, TX: Southwest Baptist Theological Seminary.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*, 180-197.

APPENDIX A

SURVEY INVITATIONS

For pilot study - this flyer accompanied a personal plea given to students in classes at MSU

Please help out a fellow Bulldog by participating in my dissertation research pilot study.

The URL below will take you to my web-based survey that is being hosted by Qualtrics. You will be asked to read the study details first. If you agree to participate in the survey, you will be asked questions about information security and will also receive a brief training session. I expect it will take you no more than 15 minutes to complete the survey. Students in course [course name] may receive [#] extra credit points by participating and completing this survey. Each student may complete the survey only once.

The survey may be accessed at this URL and will be available until [date]:

[survey URL]

Feel free to email me at lmj@msstate.edu if you have any questions. Thank you for your help!

Leigh A Mutchler
Doctoral Candidate
Department of Management &
Information Systems

For full study - this email was sent to students, faculty, and staff at MSU

This is an invitation requesting your participation in my dissertation research study.

The URL below will take you to my web-based survey that is being hosted by Qualtrics. You will be asked to read the study details first. If you agree to participate, you will be asked questions about information security and may also receive a brief training session. I expect it will take you no more than 15 minutes to complete the survey.

I have an additional favor to ask of you. Will you please forward this email to your friends, relatives, co-workers, or others you know who may be interested in helping me with my research? The only requirement is that participants must be at least 18 years of age and should each complete the survey only once. The survey may be accessed at this URL and will be available until [date]:

[survey URL]

Feel free to email me at lmj@msstate.edu if you have any questions. Thank you for your help!

Leigh A Mutchler
Doctoral Candidate
Department of Management &
Information Systems
Mississippi State University
P.O. Box 9581
Mississippi State, MS 39762

Second Recruitment - full study - this invitation accompanied invitation to AIS Membership and a Facebook posting

Please participate in my dissertation research study. It should take no more than 15 minutes of your time. The only requirement is that you must be at least 18 years of age and should complete the survey only once. Will you also ask your friends, relatives, co-workers, or others you know to participate? Use this URL to access the survey through June 30, 2012:

[survey URL]

Feel free to email me at lmj105@msstate.edu if you have any questions. Thank you for your help!

Leigh A Mutchler
Doctoral Candidate
Department of Management &
Information Systems
Mississippi State University

Third Recruitment - full study - this invitation accompanied invitation to AIS Membership

Is your information secure? Please help my PhD student with her dissertation research. You can be a part of the effort to better understand secure computing behaviors. Her study explores the relationships between the instructions provided to individuals regarding information security policies and the resulting compliance with the policies by those individuals.

Our modified "Solomon Four Group Method" requires a rather large data set and we need a few hundred more participants - can you please help us?

You may learn something about IS security, and it should take no more than 15 minutes of your time.

If you could also ask friends and others to take the survey, we'd appreciate it also.

Use this URL to access the survey: [link]

Feel free to email us at m.warkentin@msstate.edu or lmj105@msstate.edu if you have any questions. Thank you for your help!

Merrill Warkentin, Professor
Leigh Mutchler, Doctoral Candidate
Department of Management & Information Systems
Mississippi State University

APPENDIX B

SURVEY INSTRUMENT

MISSISSIPPI STATE UNIVERSITY
INFORMED CONSENT FORM FOR PARTICIPATION IN RESEARCH

We would like to ask you to participate in a research study. The purpose of this study is to attempt to better understand individual behaviors toward information security. You must be 18 years of age to participate and no discomfort or risks to participants are anticipated. The expected benefits include contributing to information security research and assisting with information security policy instructional program development. The results of this study will be analyzed and published in an academic journal; however, be assured your responses will remain anonymous.

Please note that these records will be held by a state entity and therefore are subject to disclosure if required by law. Research information may be shared with the MSU Institutional Review Board (IRB) and the Office for Human Research Protections (OHRP). For questions regarding your rights as a research participant, or to express concerns or complaints, please feel free to contact the Mississippi State University Regulatory Compliance Office by phone at 662-325-3994, by e-mail at irb@research.msstate.edu, or on the web at http://orc.msstate.edu/participant/.

If you have any questions about this research project, please feel free to contact Leigh Mutchler by email at lmj105@msstate.edu or Dr. Merrill Warkentin at 662-325-1955.

If you participate in this study, you will be asked to complete survey questions about information security topics and you may also be asked to complete a brief information security training session.

Please understand that your participation is voluntary. Your refusal to participate will involve no penalty or loss of benefits to which you are otherwise entitled. You may discontinue your participation at any time without penalty or loss of benefits.

(The following paragraph was included for the pilot study.)

Students who agree to participate in this study will be awarded ___ extra credit points for the class _____. Immediately after completing the study, students must click on the link that will close this survey and open a new survey where your name and NetID must be submitted to be awarded the extra credit.

Please take all the time you need to read through this introduction and decide whether you would like to participate in this research study.

If you wish to keep a copy of this page for your records, print it now. Should you choose to participate, clicking NEXT below will indicate your consent and take you to the next page where you will begin. It should take 10-15 minutes to complete.

NEXT

Thank you for agreeing to participate in this study!

Do you regularly use a computer that also stores personal, sensitive, or valuable information that you want protected?

□ Yes □ I'm not sure □ No

Instructions:
Please read the following about information security. When you are through, you will be asked a question. Please answer the question before continuing to the next section of this study.

Information Security Statement:
More and more information is being created and stored on computers every day, and the information is often important and valuable. Some information is personally identifying such as a Social Security number, name, address, or birth date. Other information is sensitive such as financial account numbers or health information. Yet other information may be difficult or impossible to replace such as collections of music or photographs. It is critical that all the important and valuable information stored on computers be protected from the potential threats that exist such as the one described in the following paragraph.

Electronic data loss is a very real and serious threat that can easily happen to you. Accidental file deletion, equipment failure, or equipment theft are a few common ways that make data loss very likely to happen. Experiencing data loss can cause a great deal of harm and recovering from the incident will certainly cost time and effort. The worst cases can result in losing the data forever. A recommended security response to prevent the threat of data loss is to perform data backups. A data backup is the creation of duplicate copies of electronic data so that at least two copies exist with each copy stored on a separate device. Data backups are typically performed at scheduled intervals and may include copies of the data on multiple storage media or in an on-line storage system. Performing data backups is a simple and proven way to properly protect your valuable information against the threat of electronic data loss.

Question:
Thinking about the information security statement you just read, please indicate whether the following statement is True or False.

Common causes of electronic data loss include equipment theft and accidental file deletion.
TRUE FALSE

Instructions:
Please continue by reading the following information concerning data backup training and answering a question.

Data Backup Guide:

A backup strategy should be developed and put into use to best protect against the threat of data loss. Considering the following questions related to what, where, and when can serve as a data backup guide:

1. Backup *what* data?
   - ✓ Any data that is important, valuable, or difficult to replace.
   - ✓ Examples: financial, legal, health-related records, photographs, music, e-books, etc.
   - ✓ Always have at least two copies of current data (the original plus one copy).
2. Backup to *where*?
   - ✓ Do not backup data to your local hard drive (C: drive).
   - ✓ Maintain at least one copy on storage media such as CD, DVD, external hard drive, flash drives, or others.
   - ✓ For best protection, also maintain at least one copy on an online storage system such as Dropbox, Microsoft SkyDrive, Mozy, or others.
3. Backup *when*?
   - ✓ Decide on the best backup schedule for you based on the importance of the data and on how often the data changes.
   - ✓ Example: Critical data that changes every day should be backed up every day.
   - ✓ Example: Weekly expense data should be backed up every week.
   - ✓ Example: Financial data that changes monthly should be backed up monthly.
   - ✓ Example: Photographs that never change only need to be backed up once.

Question:
Thinking about the training you just received, please indicate whether the following statement is True or False.

When considering where to back up your data, the best backup strategy includes backing up your data to your local hard drive (the C: drive).

TRUE FALSE

Instructions:

Thinking about what you just read, please indicate the amount to which you agree or disagree with each statement. Please answer each question honestly and be assured that your responses will remain anonymous.

1	2	3	4	5
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

	1	2	3	4	5
I am at risk for data loss.					
It is likely that I may lose data.					
It is possible that I may lose data.					
If I lost data, it would be a severe problem.					
If I lost data, it would be a serious problem.					
If I lost data, it would be a significant problem.					
Data backups work for protection against data loss.					
Data backups are effective to prevent data loss.					
Performing data backups will guard against data loss.					
I am confident I have the skills needed to back up data.					
I believe I have the knowledge necessary to back up data.					
I know I could successfully back up data.					
Backing up data is time consuming.					
Backing up data is a burden.					
Backing up data is inconvenient.					
People who influence my behavior think that I should perform data backups.					
People who are important to me think that I should perform data backups.					
In general, others think that I should perform data backups.					
I have experienced losing data.					
Data loss has happened to me.					
Data loss is something I have experience with.					
I have experience performing data backups.					
I have performed data backups.					
Backing up data is something I have experience with.					
I know someone who has experienced losing data.					
Data loss has happened to someone I know.					
Data loss is something others I know have experience with.					
I know someone who has experience performing data backups.					
I know others who have performed data backups.					
Backing up data is something others I know have experience with.					
I intend to backup data at least once in the next month.					
I predict I will backup data at least once in the next month.					
I plan to backup data at least once in the next month.					

Do you regularly backup your data?

□ No, never

□ Only when I am forced to (e.g., when I am running out of disk space)

□ I know I should but I don't always regularly perform backups

□ Yes, I perform data backups on a regular schedule

□ Yes, always (e.g., automatic sync to backup device or the cloud)

Instructions:
Please answer the following demographic questions:

In what year were you born? (Drop down list, select from 1922 to 1993)

What is your gender?
☐ Male ☐ Female

How many total years of computing experience do you have?
☐ Fewer than 3 years ☐ 3 to 9 years
☐ 10 to 24 years ☐ 25 or more years

What is your primary position at work or school?
☐ Student ☐ Staff
☐ Faculty ☐ Other Professional

How many total years of work experience do you have?
☐ Fewer than 3 years ☐ 3 to 9 years
☐ 10 to 24 years ☐ 25 or more years

What is the highest level of education you have completed?
☐ High School ☐ Some College
☐ Associate's ☐ Bachelor's
☐ Master's ☐ Doctoral

Primary study end.

Thank you again for your participation. When you click on Next, your answers will be submitted and the survey will end.

NEXT

Pilot study end with redirect.

Thank you again for your participation. When you click on Next, your answers will be submitted, this survey will end, and a new survey will open where you will be asked to enter your Name and NetID so that you can be awarded your course extra credit.

NEXT

[New Survey - pilot students redirecte]
Please enter your name and NetID below. Be sure you enter the information correctly so that you can be awarded be awarded ___ extra credit points for course _____.

First Name: _____ Last Name: _____

NetID _____

APPENDIX C

PRESENTATION OF ADDITIONAL FINDINGS

Table 37 Descriptive Statistics of the Primary Data Set

	N	Min	Max	Mean	Median	Std. Deviation	Skewness	Kurtosis
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic
TSU1	306	1	5	3.350	4.000	1.043	-0.565	-0.426
TSU2	306	1	5	3.131	3.000	1.072	-0.199	-0.727
TSU3	306	1	5	3.830	4.000	0.882	-1.134	1.530
TSV1	306	1	5	3.974	4.000	0.985	-0.839	0.104
TSV2	306	1	5	4.092	4.000	0.908	-1.002	0.752
TSV3	306	1	5	4.101	4.000	0.934	-1.152	1.176
REF1	306	1	5	4.320	4.000	0.679	-1.130	3.067
REF2	306	2	5	4.356	4.000	0.653	-0.875	1.198
REF3	306	2	5	4.366	4.000	0.630	-0.870	1.552
SEF1	306	1	5	4.114	4.000	0.987	-1.262	1.250
SEF2	306	1	5	4.147	4.000	0.952	-1.446	2.106
SEF3	306	1	5	4.190	4.000	0.973	-1.333	1.408
RSC1	306	1	5	3.415	4.000	1.084	-0.619	-0.393
RSC2	306	1	5	3.222	3.000	1.097	-0.285	-0.807
RSC3	306	1	5	3.196	3.000	1.151	-0.312	-0.830
SOC1	306	1	5	3.605	4.000	1.023	-0.442	-0.314
SOC2	306	1	5	3.676	4.000	0.973	-0.602	0.243
SOC3	306	1	5	3.873	4.000	0.909	-0.852	0.915
DTE1	306	1	5	3.663	4.000	1.166	-0.769	-0.459
DTE2	306	1	5	3.634	4.000	1.197	-0.718	-0.595
DTE3	306	1	5	3.673	4.000	1.184	-0.765	-0.447
DRE1	306	1	5	4.023	4.000	1.063	-1.298	1.185
DRE2	306	1	5	4.111	4.000	1.075	-1.420	1.431
DRE3	306	1	5	4.010	4.000	1.079	-1.187	0.734
VTE1	306	1	5	4.265	4.000	0.750	-1.509	4.195
VTE2	306	1	5	4.284	4.000	0.777	-1.555	3.871
VTE3	306	1	5	4.131	4.000	0.823	-1.205	2.363
VRE1	306	1	5	4.294	4.000	0.813	-1.546	3.290
VRE2	306	2	5	4.373	4.000	0.631	-0.730	0.673
VRE3	306	1	5	4.121	4.000	0.839	-1.104	1.726
BEH1	306	1	5	3.752	4.000	1.167	-0.540	-0.891
BEH2	306	1	5	3.739	4.000	1.211	-0.558	-0.911
BEH3	306	1	5	3.784	4.000	1.165	-0.600	-0.777

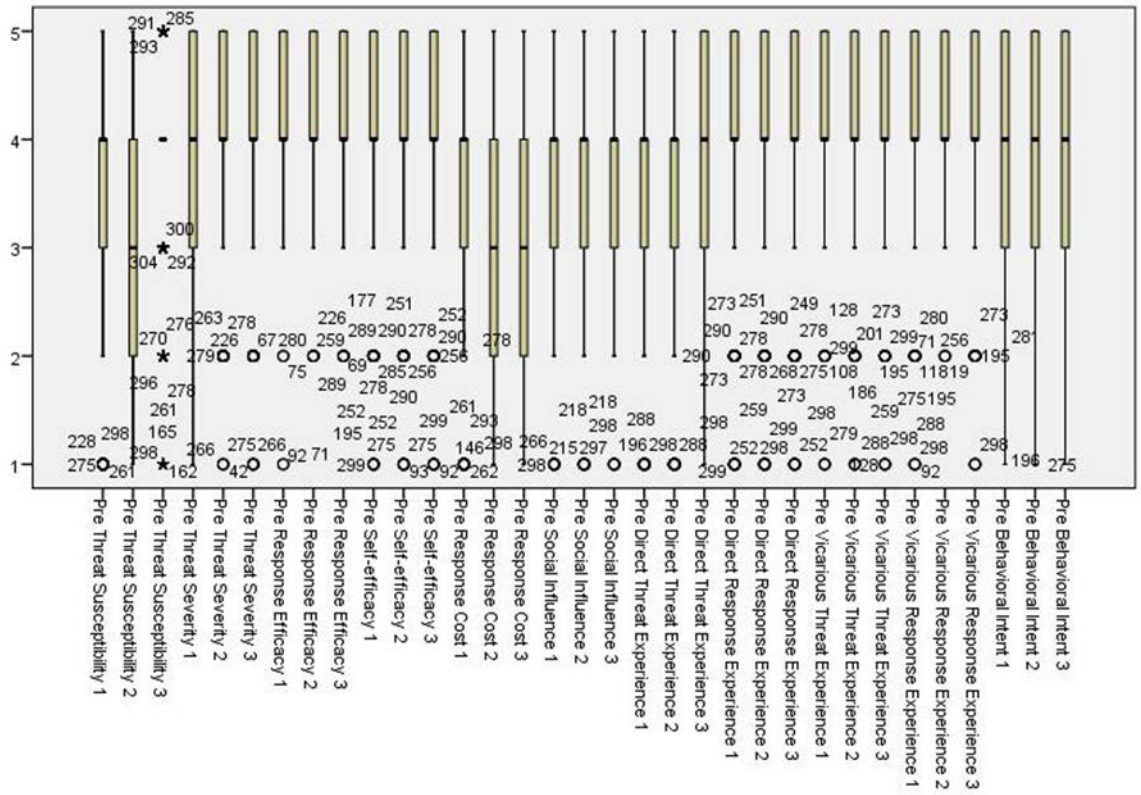

Figure 12 Primary Data Set Box Plots

Table 38 Potential Multivariate Outliers in the Primary Data Set*

Observation number	Mahalanobis D^2	p1	p2
298	150.983	0.000	0.000
275	146.748	0.000	0.000
71	117.956	0.000	0.000
196	116.096	0.000	0.000
22	108.028	0.000	0.000
146	93.282	0.000	0.000
68	88.821	0.000	0.000
138	87.416	0.000	0.000
262	87.104	0.000	0.000
159	86.838	0.000	0.000
279	86.435	0.000	0.000
14	83.230	0.000	0.000
92	80.043	0.000	0.000
256	77.031	0.000	0.000
106	76.371	0.000	0.000
292	74.564	0.000	0.000
25	71.840	0.000	0.000
233	71.608	0.000	0.000
226	70.682	0.000	0.000
259	69.384	0.000	0.000
18	67.074	0.000	0.000
195	66.176	0.000	0.000
149	62.858	0.001	0.000
160	62.653	0.001	0.000
75	62.201	0.001	0.000
228	62.193	0.001	0.000
33	60.708	0.002	0.000
97	60.698	0.002	0.000
128	57.959	0.003	0.000
288	57.133	0.004	0.000
28	56.952	0.004	0.000
162	56.893	0.004	0.000
69	56.674	0.005	0.000
212	56.242	0.005	0.000
305	56.238	0.005	0.000
42	55.294	0.006	0.000
67	53.527	0.010	0.000

*Note: Only the first 37 cases are presented here.

Table 39 Initial 10-Factor EFA Analysis Rotated Component Matrix[a]

	Component									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
TSU1									.810	
TSU2									.673	
TSU3									.835	
TSV1					.863					
TSV2					.850					
TSV3					.856					
REF1								.779		
REF2								.808		
REF3								.866		
SEF1	.857									
SEF2	.864									
SEF3	.859									
RSC1						.852				
RSC2						.884				
RSC3						.877				
SOC1							.849			
SOC2							.887			
SOC3							.765			
DTE1		.906								
DTE2		.914								
DTE3		.878								
DRE1	.840									
DRE2	.771									
DRE3	.795									
VTE1				.840						
VTE2				.830						
VTE3				.709						
VRE1										.764
VRE2				.432						.525
VRE3										.737
BEH1			.854							
BEH2			.833							
BEH3			.845							

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 7 iterations.