

5-13-2006

An Empirical Investigation Of The Influence Of Fear Appeals On Attitudes And Behavioral Intentions Associated With Recommended Individual Computer Security Actions

Allen C. Johnston

Follow this and additional works at: <https://scholarsjunction.msstate.edu/td>

Recommended Citation

Johnston, Allen C., "An Empirical Investigation Of The Influence Of Fear Appeals On Attitudes And Behavioral Intentions Associated With Recommended Individual Computer Security Actions" (2006). *Theses and Dissertations*. 509.
<https://scholarsjunction.msstate.edu/td/509>

This Dissertation - Open Access is brought to you for free and open access by the Theses and Dissertations at Scholars Junction. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Scholars Junction. For more information, please contact scholcomm@msstate.libanswers.com.

AN EMPIRICAL INVESTIGATION OF THE INFLUENCE OF FEAR
APPEALS ON ATTITUDES AND BEHAVIORAL INTENTIONS
ASSOCIATED WITH RECOMMENDED
INDIVIDUAL COMPUTER
SECURITY ACTIONS

By

Allen C. Johnston

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

Mississippi State, Mississippi

March 2006

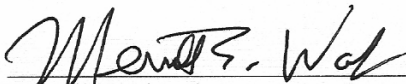
Copyright by
Allen C. Johnston
2006

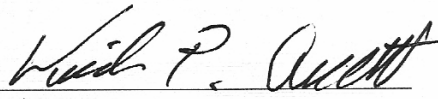
AN EMPIRICAL INVESTIGATION OF THE INFLUENCE OF FEAR
APPEALS ON ATTITUDES AND BEHAVIORAL INTENTIONS
ASSOCIATED WITH RECOMMENDED
INDIVIDUAL COMPUTER
SECURITY ACTIONS

By

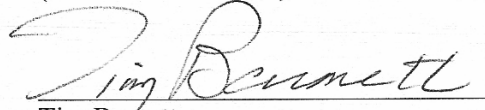
Allen C. Johnston

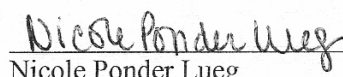
Approved:

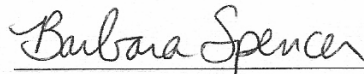

Merrill Warkentin
Professor of Management
Information Systems
(Chair Dissertation Committee)

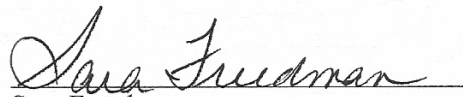

Kirk Arnett
Professor of Management
Information Systems
(Committee Member)


Steve Taylor
Professor of Management
(Committee Member)


Tim Barnett
Professor of Management
(Committee Member)


Nicole Ponder Lueg
Assistant Professor of Marketing
(Committee Member)


Barbara Spencer
Director of Graduate Studies in
the College of Business and Industry


Sara Freedman
Dean of the College of Business and Industry

Name: Allen C. Johnston

Date of Degree: May 13, 2006

Institution: Mississippi State University

Major Field: Business Information Systems

Major Professor: Dr. Merrill Warkentin

Title of Study: AN EMPIRICAL INVESTIGATION OF THE
INFLUENCE OF FEAR APPEALS ON ATTITUDES AND
BEHAVIORAL INTENTIONS ASSOCIATED WITH
RECOMMENDED INDIVIDUAL COMPUTER SECURITY
ACTIONS

Pages in Study: 175

Candidate for the Degree of Doctor of Philosophy

Through persuasive communication, IT executives strive to align the actions of end users with the desired security posture of management and of the firm. In many cases, the element of fear is incorporated within these communications. However, within the context of computer security and information assurance, it is not yet clear how these fear-inducing arguments, known as fear appeals, will ultimately impact the actions of end users.

The purpose of this study is to examine the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions toward the amelioration of threats. A two-phase examination was adopted that involved two distinct data collection and analysis procedures, and culminated in the development and testing of a conceptual model representing an infusion of theories based on prior research in Social Psychology and Information

Systems (IS), namely the Extended Parallel Process Model (EPPM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). Results of the study suggest that fear appeals do impact end users attitudes and behavioral intentions to comply with recommended individual acts of security, and that the impact is not uniform across all end users, but is determined in part by perceptions of self-efficacy, response efficacy, threat severity, threat susceptibility, and social influence. The findings suggest that self-efficacy and, to a lesser extent, response efficacy predict attitudes and behavioral intentions to engage individual computer security actions, and that these relationships are governed by perceptions of threat severity and threat susceptibility.

The findings of this research will contribute to IS expectancy research, human-computer interaction, and organizational communication by revealing a new paradigm in which IT users form perceptions of the technology, not on the basis of performance gains, but on the basis of utility for threat amelioration.

DEDICATION

I would like to dedicate this research in celebration of Mississippi State University, its valuable contributions to higher education and to an immeasurable number of lives.

ACKNOWLEDGEMENTS

I would like to extend my sincere gratitude to the members of my committee, who so willingly guided my efforts in completing this study. Dr. Kirk Arnett generously provided his extensive insight into information systems theory and, in particular, information assurance. Dr. Nicole Ponder Lueg tirelessly guided and evaluated the quantitative aspects and overall quality of the work. Drs. Steven Taylor and Tim Barnett assisted me throughout the process, lending their valuable expertise in research design.

My deepest appreciation and admiration goes to Dr. Merrill Warkentin, the chair of the dissertation committee, my academic mentor, and close friend. My decision to enter the doctoral program in 2003 is directly correlated with his arrival at Mississippi State University, as it was his teachings and works in the field that first drew my interest to the academic arena. Through his leadership and guidance, I have been provided with the resources necessary to successfully complete this program. I will forever be grateful to him.

Finally, I would like to thank my wife, Michelle, and my two little girls, Rae and Abby, whose love, support and understanding through this journey has been remarkable. Also, I owe a great deal to our parents, Richard and Sue Johnston and Paul and Freida Buckley, who extended the helping hands that turned this dream into a reality.

TABLE OF CONTENTS

	Page
DEDICATION	ii
ACKNOWLEDGEMENTS	iii
LIST OF TABLES	vii
LIST OF FIGURES	ix
CHAPTER	
I. INTRODUCTION.....	1
Persuasive Communications	7
Fear Appeals	8
Acceptance Models.....	14
Source Credibility	16
Overview of the Conceptual Research Model	17
Research Objective	20
Research Methods.....	22
Significance of the Study.....	23
Organization.....	24
II. LITERATURE REVIEW.....	27
Fear Appeals Defined	27
Fear	30
Threat.....	32
Efficacy	33
Fear Appeals Research Overview.....	34
Primary Fear Appeal Theories and Models	36
Drive Models	36
Parallel Process Model.....	37
Protection Motivation Theory.....	39
Extended Parallel Process Model.....	40
Fear/Threat Relationship.....	43
Acceptance Models.....	44
Source Credibility	54
Research Model and Hypotheses Development	56
Outcomes of the Model.....	58
Attitude	59
Determinants of Attitude.....	61
Moderating Effect of Perceived Threat.....	65
Threat Severity.....	65

CHAPTER	Page
Threat Susceptibility	66
Relationships between Source Credibility and Perceptions of Threat and Efficacy	67
Source Competence	67
Source Trustworthiness.....	68
Source Dynamism.....	69
Summary	70
 III. RESEARCH METHODS.....	 71
Variables	71
Instrument Design.....	73
A Two-Phase Investigation.....	79
Preliminary Investigation.....	80
Experimental Treatment Content Validity.....	80
Instrument Content Validity	84
Construct Validity and Reliability	85
Pilot Study.....	86
Primary Investigation.....	86
Experimental Design.....	89
Experimental Procedure.....	92
Sampling Frame	94
Summary	96
 IV. DATA ANALYSIS AND RESULTS	 97
Preliminary Investigation Results	97
Exploratory Factor Analysis	98
Primary Investigation Results.....	101
Characteristics of the Sample.....	101
Tests of Internal and External Validity.....	104
The Measurement Model	106
Specification and Respecification of the Measurement Model	108
Scale Assessment and Validation	109
The Structural Model	113
Tests of the Hypotheses	113
Interpretation.....	120
Post Hoc Analysis.....	128
Respecification of the Structural Model	128
Interpretation.....	132
Summary	136
 V. DISCUSSION AND CONCLUSION.....	 138

CHAPTER	Page
Implications of IS Theory	139
Implications of IS Practice.....	142
Limitations	144
Future Research	147
REFERENCES	149
APPENDIX	
A. EXEMPLAR FEAR APPEALS.....	162
B. SURVEY INSTRUMENT	169
C. FEAR APPEAL TREATMENT	174

LIST OF TABLES

TABLE	Page
1.1 IT Support Activity Responsibilities Across IT Governance Continuum	6
1.2 Fear Appeal Origins, Motivation, and Examples	14
2.1 Fear Appeal Research, Significance and Theoretical Advancement	35
3.1 Dependent Variables of Interest	72
3.2 Determinants of Attitude	74
3.3 Factor Loadings for Scale Items Used to Measure Threat Severity, Threat Susceptibility, Response Efficacy, and Self-efficacy	76
3.4 Factor Loadings for Scale Items Used to Measure Social Influence, Performance Expectancy, Attitude, and Behavioral Intent	78
3.5 Factor Loadings for Scale Items Used to Measure Source Competence, Source Trustworthiness, and Source Dynamism	79
3.6 Experimental Treatment Fear Appeal Components	82
3.7 Hypotheses and Model Estimation Components	87
4.1 Verimax Rotated Component Matrix	100
4.2 Respondent Demographic Information	103
4.3 Between Subjects ANOVA for Groups One and Two	104
4.4 Between Subjects ANOVA for Groups Three and Four	105
4.5 Between Subjects ANOVA for Groups One and Three	106

TABLE	Page
4.6 Between Subjects ANOVA for Groups Two and Four	106
4.7 Measurement Model Specification Process	109
4.8 Confirmatory Factor Analysis	111
4.9 Reliability, AVE and Inter-Construct Correlations	112
4.10 Measurement Model Re-Specification Process	113
4.11 Standardized Path Estimates for Proposed Structural Model	115
4.12 Comparison of Structural Models with High/Low Threat Severity	117
4.13 Tests of Threat Severity as Moderating Variable	118
4.14 Comparison of Structural Models with High/Low Threat Susceptibility	119
4.15 Tests of Threat Susceptibility as Moderating Variable	120
4.16 Hypotheses and Model Estimation Components Testing Results	121
4.17 Model Re-Specification Process for Structural Model	129
4.18 Standardized Path Estimates for Re-Specified Structural Model ..	130
4.19 Comparison of Re-Specified Structural Models with High/Low Threat Severity	131
4.20 Tests of Threat Severity as Moderating Variable	131
4.21 Comparison of Re-Specified Structural Models with High/Low Threat Susceptibility	132
4.22 Tests of Threat Susceptibility as Moderating Variable	132

LIST OF FIGURES

FIGURE	Page
1.1 The Security Action Cycle	4
1.2 Fear Appeal Assessment Outcomes	11
1.3 Conceptual Research Model	19
2.1 Extended Parallel Process Model	41
2.2 Technology Acceptance Model (TAM)	47
2.3 TAM2	49
2.4 Unified Theory of Acceptance and Use of Technology (UTAUT) ...	52
2.5 Conceptual Research Model	57
3.1 Solomon Four-Group Design	92
4.1 The Structural Model	116
4.2 The Respecified Structural Model	134
4.3 Structural Model with Only Significant Paths	135

CHAPTER I

INTRODUCTION

Within the modern business climate, threats to corporate data, information technology (IT) infrastructure, and personal computing interests pervade. According to the 2004 Computer Crime and Security Survey conducted jointly by the Computer Security Institute (CSI) and the San Francisco Office of the Federal Bureau of Investigation (FBI), 53% of respondents reported that their organization experienced some form of malicious attack during the past year (Gordon, Loeb, Lucyshyn, & Richardson, 2004). But this figure may understate the magnitude of the problem in that many organizations refuse to comment on questions regarding their information assurance practices and security breach history due to investor confidence interests and in order to maintain a low profile.

Based on responses obtained from a sample of 494 security practitioners from government, financial, medical, business, and higher education institutions, the most frequently reported forms of malicious attack are virus attacks and insider abuse at a reported rate of 78% and 59%, respectively (Gordon et al., 2004). Within the realm of these respondents, costs associated with virus attacks were determined to be \$55 million, while insider abuse costs were over \$10 million. Interestingly, denial of service (DoS) attacks, while only reported by 17% of the respondents, resulted in losses of

approximately \$26 million. One of the damaging outcomes of many forms of malware is that of identity theft. According to statistics reported by the Federal Trade Commission, 27.3 million Americans reported identity theft victimization in a five-year period beginning in October of 1998 and ending in October of 2003 ("Cybercrime: Expansive and Expensive," 2005). The financial losses felt by businesses and financial institutions over that same time period were estimated at \$48 billion ("Cybercrime: Expansive and Expensive," 2005).

Threats to computing environments may originate from either internal or external sources and from human or non-human sources. Also, specific instances of these threats may occur intentionally or accidentally (Loch, Carr, & Warkentin, 1992). In a study conducted by Luftman and McLean (2004), 301 information technology (IT) executives were surveyed as to their most pressing management concerns. Of the five top concerns, security and privacy ranked third, with CIOs placing it higher on average than other executives. Luftman and McLean argue the high ranking is a result of post 9/11 concerns as well as a general movement among consumers to demand "greater protection from identity theft and other privacy threats." (p. 90).

Regardless of where the threats originate, their characteristics, including frequency, severity, and monetary impact, have become significant enough to attract the attention of high-level administrators (Whitman, 2003) as well as those charged with securing the enterprise (Straub & Welke, 1998). A major focus of this charge concerns efforts to provide effective endpoint security (Rasmussen, 2004). Endpoint security refers to the collection of policies, procedures, and subsequent actions directed at

securing the perimeter of the organization. It is the domain of the end user. As such, the challenges facing IT managers in providing effective endpoint security are unique in that they may rely heavily on end user participation.

The degree to which technology professionals can align the actions of end users with the goals of information assurance will ultimately dictate the level of success their organization has in coping with the threats (Straub & Welke, 1998). IT professionals strive to instill a consistent approach to endpoint security through policies and procedures that govern end user computing. Security management is an especially challenging area in this respect in that end users are not consistent in their level of threat awareness, knowledge, or efficacy for effectively controlling their respective computing facilities. The fact that there usually exists a large differential among end users in terms of access privileges, priority, and motivation further complicates compliance efforts.

Straub and Welke (1998) argue that the relationship between managers and their end user community is reflective of the application of general deterrence theory. This theory suggests that the actions of managers are critical to the successful deterrence, prevention, detection and remediation of security risks. As depicted in Figure 1.1, the security action cycle establishes these actions as sequential events whereby the outcome of one line of defense dictates the next.

Deterrence actions refer to a class of proactive techniques, such as acceptable use policies and general computing guidelines, which are intended to minimize the potential for security breaches (Straub & Welke, 1998). Effective communication between managers and end users is an important condition for successful deterrence. If deterrence

strategies are ineffective, then preventive measures such as access controls must be utilized (Straub & Welke, 1998). These measures could be regarded as enforcement techniques for deterrence strategies. If preventive measures fail, the next sequential phase of the security action cycle is detection (Straub & Welke, 1998). Detection mechanisms are intended to identify security intrusions and establish evidence for possible counteractions. The last phase in the cycle is referred to as the remedy phase. Within this phase, actions are taken to recover from detected security risks (Straub & Welke, 1998). Obviously, if remedy actions are employed, deterrence and preventive actions were either late or ineffective.

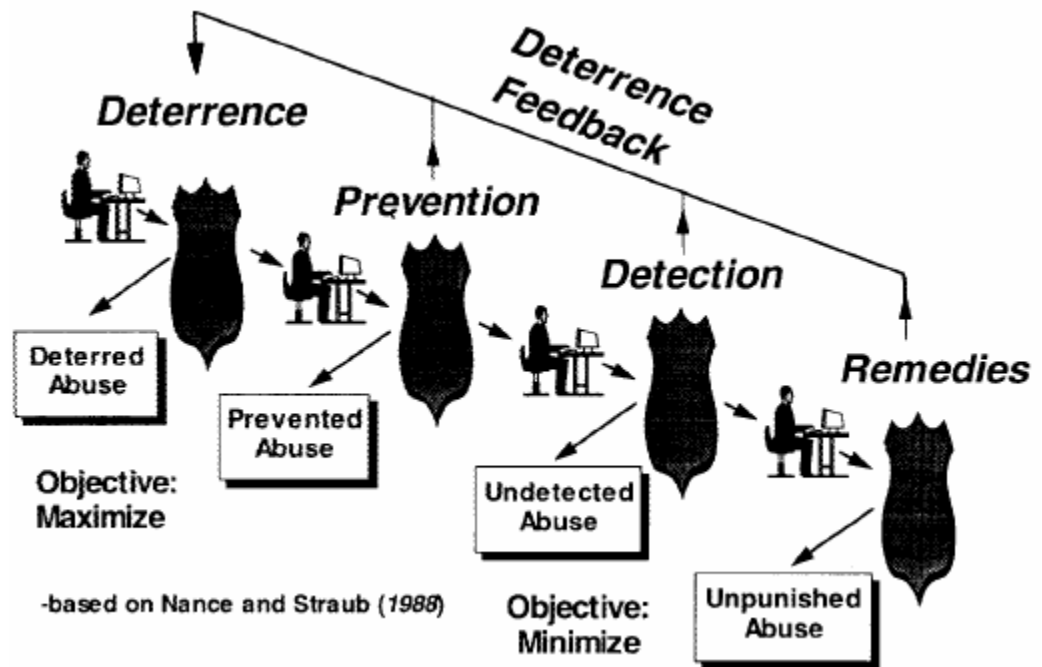


Figure 1.1

The Security Action Cycle

An important element in the success of any phase in this cycle is the degree to which managers are able to influence their constituents. Managerial influence over end users is dependent upon the autonomy end users enjoy within their respective IT environments. For those end users operating within environments that are considered to be highly centralized, their interaction with IT managers is limited as the majority of computing support operations are handled by a single administrative unit. As depicted in Table 1.1, end user responsibilities toward the support of their IT interests can be considered along a continuum ranging from highly centralized to highly decentralized environments.

End users operating in decentralized environments in which they share or maintain sole responsibility for their computing resources commonly receive input from others as to the most effective practices. The intention of this input is to steer the end user action in a direction that is consistent with the goals management or the firm, in general. For high-level managers desiring reliable responses from their end user community in response to a security threat, the use of persuasive arguments is especially appealing.

Generally speaking, the present study investigates the effectiveness of persuasive messages in motivating end users to take action to secure their respective computing interests. Specifically, the persuasive messages of interest are those that include the element of threat, so often found in secure computing literature (see Appendix A). These types of persuasive messages are referred to as *fear appeals* and have been the subject of numerous studies across a wide variety of domains. In order to facilitate this research, a

specific type of threat is examined that is consistent with those encountered in environments in which end users have some degree of autonomy over their computing resources. This specific threat is the increasingly notorious malware known as spyware.

Table 1.1 IT Support Activity Responsibilities Across IT Governance Continuum

IT Support Activity	Centralized	Decentralized
virus protection	maintained by central administrative unit	end users are responsible for their own virus protection
access controls	global controls established by central administrative unit	local controls established by end users
firewall protection	maintained by central administrative unit	end users maintain personal firewall solutions
media backup	central administrative unit is solely responsible for initiating and monitoring all data redundancy procedures	end users are responsible for personal media backup
employee education	formal training programs are developed and implemented by central administrative unit	end users are responsible for handling their specific training needs
audit procedures	central administrative unit monitors all relevant system and network logs	end users monitor their own systems for inappropriate activities
workstation control	only central administrative unit maintains administrative rights of workstations	end users maintain administrative rights to their respective workstations
software deployment	software is deployed only through centralized process	end users are responsible for software installation
host intrusion detection	central administrative unit is solely responsible for host intrusion detection	end users are responsible for personal host intrusion detection

Spyware is an appropriate proxy for those threats found in autonomous computing environments because of the nature by which it propagates, maintains and is removed. While centrally controlled virus protection mechanisms are prevalent in the majority of organizations, spyware remains a threat that is addressed on an individual basis. Currently, few enterprise solutions for spyware amelioration exist, and for those that do, the technology has not progressed to the level of robustness and stability found in anti-virus programs.

The remainder of this chapter provides an overview of persuasive communications, and fear appeals in particular, followed by descriptions of the theories of acceptance models and source credibility. Cumulatively, these theories serve as the underpinning of a conceptual research model that seeks to explain and predict the influence that fear appeals have on attitudes about spyware threats and subsequent behavioral intentions for amelioration. An overview of the conceptual research model, the objective of this research, and its associated research questions are described, followed by statements as to the significance and organization of the study.

Persuasive Communications

Fishbein and Ajzen (1975) contend that persuasive communications are an effective method for modifying human attitudes, intentions, and behaviors. Siponen (2000) recommends the use of persuasion in security management, specifically citing emotions as a leverage point from which persuasive messages can “affect attitudes and motivation in a positive manner” (p. 37). Persuasive arguments can be found within various artifacts to which end users are exposed. For example, persuasive messages may

exist within the very policy and procedure documents that govern the computing activities of an organization's employees. Also, persuasive messages may be embedded within the software applications utilized by end users and triggered by either logic or time. One frequently encountered persuasive message is that generated by anti-spyware applications. These programs warn end users to update their spyware definitions in order to avoid potential negative risks associated with spyware activity. The goal of this communication is to engender compliance with a particular procedure by pointing out the negative consequences associated with noncompliance.

As Straub and Welke (1998) describe, there are many factors that influence compliance. The threat of negative sanctions is one that is widely used within computing environments to encourage responsible computer usage. Alternatively, positive reinforcement techniques, such as incentive programs, employee empowerment (when desired), as well as general praise, are often employed to convey the importance of security actions. Additionally, training programs, brochures, reminder bulletins, and calendar or email alerts are utilized in an attempt to promote awareness and knowledge. However, the ultimate threat of reprimand, such as account denial, privilege removal or increased supervision of activities, has become standard practice for compliance encouragement.

Fear Appeals

The use of fear appeals as a form of persuasive communication is gaining momentum as a technique for eliciting a compliance response for personal security action (Whaley, 2005). The goal of a fear appeal is to motivate a behavioral change by

leveraging the primitive, natural emotion of fear associated with the perception of a threat. Once a threat is perceived as personally relevant and dangerous, an end user will then consider actions to either address the threat or their fear.

Fear appeals have often been utilized within the healthcare sector to motivate individuals to think or behave in a manner that is consistent with what is considered to be “safe.” Examples of fear appeals in healthcare include public service announcements concerning HIV and AIDS awareness (Casey, 1995), drug abuse (Dillard, Plotnick, Godbold, Freimuth, & Edgar, 1996), drinking and driving, and skin cancer (Stephenson, 1993). In a study involving female college students, women provided with coping information to detect and avert breast cancer were found less likely to engage in maladaptive behavior (Fry & Prentice-Dunn, 2005). Fear appeals have also been applied to other fields of interest including public service. For instance, Hovland, Janis and Kelly (1953) describe the use of fear appeals by government officials to summon support for national defense initiatives by underlining the dangers associated with being unprepared. Another example can be found in the use of fear appeals in television advertisements by the U.S. Office of National Drug Control Policy to raise awareness of drug use among America’s youth (Dejong & Wallack, 1999). The underlying element in all of these types of communications is the fact that they play upon the emotion of fear; the fear of being injured, causing injury to others, becoming ill, or dying.

In addition to the content associated with depicting a relevant and severe threat, a fear appeal will also contain a feasible *recommended response* to avert the threat. Within the context of computer security, a recommended response may describe a procedure

involving a sequential series of individual actions to address a threat. Some actions may be strictly behavioral, while others may involve the use of a particular technology necessary to avert a threat. An example of technology use could be the application of anti-virus programs to detect and eliminate virus or worm infestations. An example of a behavioral action could be the filtering of unsolicited emails.

An individual's attitude, behavioral intent, and behavior regarding the recommended response is an indication of whether he or she has accepted or rejected the fear appeal message. *Message acceptance* is the typical outcome in a fear appeal assessment and is gauged by measures of attitude, behavioral intention, and behavior toward the recommended response (Witte, 1992). When an individual is described as having engaged in message acceptance, this means the individual has responded with positive attitudes, intentions and behaviors toward the message recommendations. *Message rejection* is an alternative outcome of a fear appeal assessment. Message rejection refers to coping responses intended to reduce fear and can be assessed by any of three alternative reactions: (a) aggression toward the source of the message; (b) defensive avoidance; or (c) inattentiveness to the message, whereby an individual denies that he or she is at risk for a certain threat. Figure 1.2 depicts fear appeal assessment as described above.



Figure 1.2

Fear Appeal Assessment Outcomes

One conventional fear appeal theory, the Fear-as-Acquired Drive Model (Hovland, Janis, & Kelly, 1953; Janis, 1967), established that threat awareness, in conjunction with guidance for threat amelioration, may engender a protection response consistent with the goals of the advice as long as the advice was successful in reducing the negative emotions associated with fear. Alternatively, threat awareness in the absence of effective advice or guidance fosters a culture of defensive avoidance. This model was further refined by Leventhal's (1970) Parallel Process Model (PPM), Rogers' (1975) Protection Motivation Theory (PMT) and later, Witte's (1992) Extended Parallel Process Model (EPPM) to consider not only the efficacy of the response but also the efficacy of the individual performing the recommended action. EPPM benefits from the refinement of previous theories and models. As such, EPPM is firmly established in psychological literature as a valid and reliable model for explaining the influence of fear appeals on attitudes and intentions (Roskos-Ewoldsen, Yu, & Rhodes, 2004).

From a technological perspective, fear appeals are engineered to influence the attitudes, intentions and behaviors associated with the acceptance of a recommended response to avert a threat to computing resources. These recommended responses are procedures that serve either to provide (a) guidance for deterring a threat; (b) preventive measures for averting a threat; (c) guidance for detecting a previous infection; or (d) responsive direction for recovering from a previous infection. Under any of these conditions, the recommended response involves actions to mitigate a perceived threat. However, when fear appeals lack directions to mitigate the associated threat, the effect may be realized in the form of inhibited technology usage or technology avoidance.

Fear appeals can originate from social influences such as organizational leaders, technological leaders, and trusted colleagues. These fear appeals may be verbalized through formal or informal conversation or they may be documented in spirit within policy and articulated more clearly in procedure. Once the procedures are instantiated in practice, the influence of fear appeals as behavior modifiers becomes apparent. For upper-level technology managers of an organization that wish to include fear arousing persuasive messages within their acceptable use documents, apart from empirical tests of attitude and behavioral intent, the only indication of fear appeal success would be observed employee behavior.

Within the computer security software vendor community, the use of fear appeals to influence the adoption of their products is not novel. In fact, a growing trend among purveyors of information assurance and computer security technology is to employ fear-arousing messages to provoke a favorable behavioral response among existing and

potential clientele (Whaley, 2005). A favorable response may be realized in the form of product selection and purchase, adoption or diffusion throughout a firm or industry.

There are numerous fears associated with technology use which security technology purveyors leverage to cast a shadow of insecurity within the users community (Whaley, 2005). Fear of the unknown, the unattained, the incomplete, the obsolete, the unregistered and the underutilized are just a few of the fears that these communication elements seek to exploit in order to solicit attention to their product and an associated response that will ultimately lead to product dependence. Once dependent, the user will consider fewer alternative solutions and will more readily agree to renew product licenses.

It is common practice for security technology vendors to place fear appeals in product documentation such as “Best Practices” or “FAQs.” This form of fear appeal has the added benefit of residing in a location typically associated with installation guides and reference materials, thereby providing warnings and instructions for coping with the threats at a particularly vulnerable moment for the user. Table 1.2 provides a description of the sources of fear appeals, their motivation, and examples.

Table 1.2 Fear Appeal Origins, Motivation, and Examples

Source	Motivation	Examples (Appendix A)
purveyors of computer security technology	to persuade potential and existing customers to purchase, implement or continue to use their products	<ul style="list-style-type: none"> - McAfee Hoaxes - McAfee AntiSpyware - Webroot's Spyware Sweeper - Microsoft AntiSpyware
organizational technology leaders (CIO/CTO/CSO)	to raise awareness and influence behaviors among the users within their organizations toward safe computing	<ul style="list-style-type: none"> - logout after use - avoid opening attachments containing .vbx extensions - turn off remote administrator service - do not send passwords in clear text
trusted colleagues	to encourage behaviors consistent with the social norm	<ul style="list-style-type: none"> - use encryption software - don't share passwords
news media	to raise awareness among general population of the present dangers to safe computing	<ul style="list-style-type: none"> - coverage of growing identity theft epidemic

Acceptance Models

Much prior research in the social, psychological, and behavioral sciences has been devoted to the study of the antecedents of technology acceptance and use. The early works of Fishbein and Ajzen (1975), Davis (1989), and Compeau and Higgins (1995b) established attitude and behavioral intention as indicators of an individual's acceptance and use of technology. In fact, Davis' Technology Acceptance Model (TAM) was the first to model *perceived usefulness* and *perceived ease of use* as predictors of behavioral intention specifically within the context of information technologies. Based primarily on Fishbein and Ajzen's Theory of Reasoned Action (TRA), TAM has been instrumental in

the development of future models that have increased our ability to predict technology acceptance and use.

Acceptance models continued to evolve and increase in predictive ability and complexity. For instance, Venkatesh and Davis (2000) introduced TAM2 as an extension of TAM through the incorporation of subjective norms into the model. Other models utilized in the study of behavioral intent include the Motivational Model (MM), the Theory of Planned Behavior (TPB), the Combined Theory of Planned Behavior and TAM (C-TPB-TAM), the Model of PC Utilization (MPCU), the Social Cognitive Theory (SCT), and the Innovation Diffusion Theory (IDT). Each of these theories provided their own unique contribution to the research stream and were ultimately combined to form today's most intriguing IS acceptance model, the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis, & Davis, 2003).

UTAUT represents a current synthesis of the eight complementary models listed previously. The eight original models were only able to explain anywhere from 17% to 53% of the variance in behavioral intent (Venkatesh et al., 2003). Based on analysis of data collected from four organizations over a six-month period with three distinct points of measurement, the UTAUT model was able to explain up to 69% of the variance in behavioral intent (Venkatesh et al., 2003). The UTAUT model provides both academicians and practitioners with the ability to investigate influential factors such as *performance expectancy*, *effort expectancy*, *social influence*, and *facilitating conditions* in light of gender, age, experience with the technology, and voluntariness of use toward the behavior intentions and usage behavior associated with a technology.

UTAUT provides a theoretical foundation for explaining end users' intentions to adopt a recommended individual computer security action as dictated within a fear appeal. Because UTAUT describes actions involving technological advances, it is able to explain end users' intentions to adopt a recommended course of action involving computer security if extended appropriately with a contemporary fear appeal theory. Therefore, by integrating UTAUT with EPPM, it is possible to apply the combined model within the domain of information assurance to account for the perception of threat and efficacy associated with decentralized computing environment threats such as spyware.

Source Credibility

Prior research suggests that high-credibility sources are more influential in modifying an individual's attitudes and behaviors than low-credibility sources (Hovland & Weiss, 1951; Maddux & Rogers, 1980; Wittaker & Meade, 1968). Therefore, it is expected that a communication that originates from the office of the Chief Information Officer (CIO) or Chief Security Officer (CSO) will have a greater chance of instilling a perception of a relevant and severe threat than if the message came from a clerk in the mailroom. Although fear appeal and source credibility research streams are conceptually linked to the investigation of the influence of persuasive messages, they are not frequently addressed in the same research. Intuitively, it is easy to recognize however, that when communicating a recommended course of action in response to a severe and probable danger, the source of the appeal will influence its audience's perceptions and resultant attitudes and behavioral intentions.

Overview of the Conceptual Research Model

Figure 1.3 shows the conceptual model used in this study to explain and predict the influence of fear appeals on attitudes and behavioral intentions to adopt recommended individual computer security actions. As the applicability of fear appeals in this context is limited to conditions where individuals have alternatives to the suggested actions, it is reasonable to describe the environment of this study as decentralized or federated. Both of these forms of IT governance provide a degree of autonomy to the end user necessary for influential arguments such as fear appeals to be relevant.

The conceptual model represents an integration of three theories from fear appeals, acceptance models, and source credibility research as described above. All of the constructs of EPPM are included in the conceptual model. All of the UTAUT constructs except effort expectancy and facilitating conditions are included in the conceptual model. Effort expectancy is not included since the underlying perception that it is designed to capture is found within the self-efficacy construct in EPPM. Facilitating conditions is not included because it is a determinant of behavior which is not within the scope of this study. Finally, the constructs borrowed from the source credibility literature are those which are included in the Leathers Personal Credibility Scale (Leathers, 1992). While one of several scales available for measuring source credibility, the parsimonious nature of the scale and its proven reliability (Powell & Wanzenried, 1995) warrants its use.

The outcomes of the conceptual model are attitude and behavioral intent. These outcomes are indicators of the effectiveness of fear appeals in affecting human cognitions

and emotions concerning recommended individual protective actions. Attitude is a determinant of behavioral intent. Antecedents of attitude are perceptions of response efficacy, self-efficacy, performance expectancy and social influence. Response efficacy and self-efficacy are based on Witte's fear appeal model, EPPM, while performance expectancy and social influence are borrowed from UTAUT. The relationships between these antecedents and attitude are moderated by perceptions of threat severity and threat susceptibility as described in EPPM. The perceptions of threat severity and susceptibility are influenced by the three antecedent factors of source credibility as described by the Leathers Personal Credibility Scale: source competency, source trustworthiness, and source dynamism. Source competency and source trustworthiness also influence response efficacy.

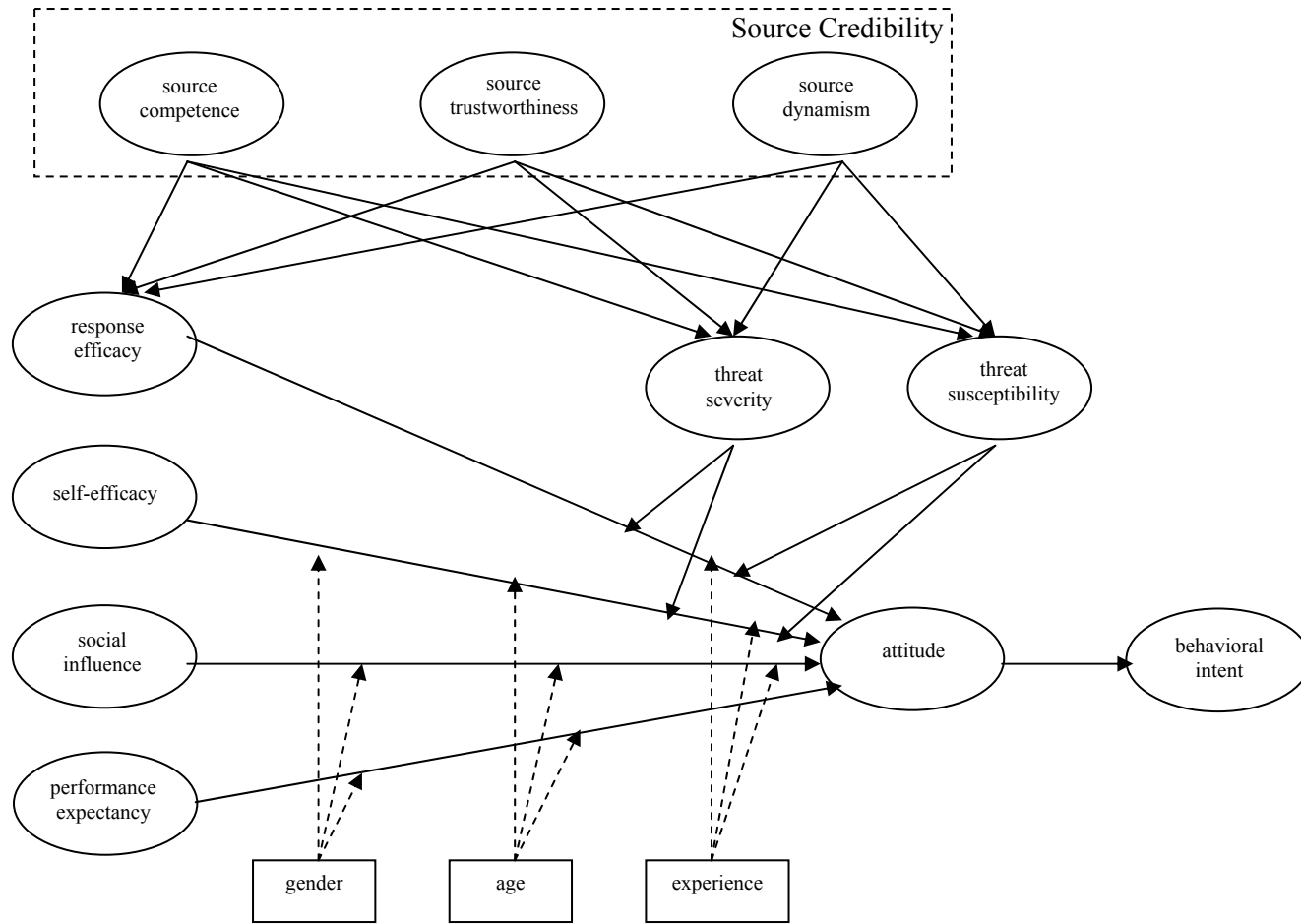


Figure 1.3

Conceptual Research Model

Research Objective

The purpose of this study is to examine the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions toward the amelioration of threats. Through the investigation of fear appeals concerning the specific threat of spyware, it is expected that the findings will be generalizable to include all computer security threats within decentralized environments. The decentralized constraint is necessary because the purpose of a fear appeal is to affect change through persuasion, which is not facilitated by the mandatory or automated circumstances found in centralized environments.

Toward the pursuit of this purpose, one primary research question and several supplementary questions are posed to articulate the issues concerning fear appeal use and acceptance model deficiencies within the context of individual computer security management. The primary research question to be addressed in this study is:

How do fear appeals modify end users' attitudes and behavioral intentions associated with recommended individual computer security actions?

UTAUT provides an established model for explaining end users' intentions to adopt a new technology. By applying this model within the domain of computer security, new constructs are merged with those established by Venkatesh et al. (2003) to create a conceptual model capable of predicting end user attitudes and intentions to adopt a recommended course of action as advocated in a fear appeal. In testing this conceptual model, however, the following questions will be answered that relate specifically to the validity of UTAUT within this unique context:

How do end users' attitudes toward a recommended individual computer security action influence their intentions to adopt the recommended action?

How do end users' perceptions of the support provided by their friends and colleagues to perform a recommended individual computer security action influence their attitudes toward the recommended action?

How do end users' expectations of performance afforded by a recommended individual computer security action influence their attitudes toward the recommended action?

In examining the fear appeal component of the research purpose, the following subordinate questions are posed that serve to focus the study:

How do end users' perceptions of the efficacy of a recommended individual computer security action influence their attitude to adopt the recommended action?

How do end users' perceptions of their ability to perform a recommended individual computer security action influence their attitude to adopt the recommended action?

In determining end users' attitudes toward a recommended individual computer security action, do perceptions of threat severity and threat susceptibility govern their perceptions of efficacy?

How does source credibility impact the effectiveness of a fear appeal in altering end users' attitudes and intentions regarding a recommended individual computer security action?

As previously stated, these issues will be explored via a proxy for computer security threats and subsequent threat amelioration actions. Spyware will serve as a specific instance of threat that has the properties consistent with those found in decentralized or federated environments.

Research Methods

Toward fulfilling the objective of this research, numerous obstacles to the validity of the research were identified and addressed. Specifically, this study involved the development and testing of a model to explain user attitudes and intentions toward computer security actions as recommended through emotionally charged persuasive communications. The persuasive communications took the form of a typed document supplemented with a streaming video of a credible source of computer security management advice. To adequately ensure that the fear appeal treatment was the impetus of change in attitude and behavioral intent, a Solomon four-group experimental design was employed. The Solomon four-group design enabled the researcher to control for threats to internal and external validity. Considering the nature of this experiment, it was especially necessary to ensure that the testing conditions were not interacting with the stimulus.

The sample for this research consists of faculty, staff, and students from Mississippi State University. The context of this study is individual computer security management; as such, it is desirable to gauge the perspectives of technology users that have a vested interest in protecting their personal digital assets. Mississippi State University provides a computing environment that encourages individual autonomy for the security of end user computing facilities. Moreover, the threat of spyware is addressed by the technology leaders of the University through persuasive arguments advocating individual actions involving anti-spyware software procedures. There are, however, certain environments within the University that discourage end user autonomy,

and that implement IT policy and procedures through a central administrative unit. Therefore, the participants in this study were initially screened via three questionnaire items. The items were intended to ensure each participant had access to at least one computer system within which he or she maintained important data and was at least partially responsible for the security of the system. Assuming the participants met these criteria, their perspectives were expected to be generalizable to the greater population of autonomous technology users.

Significance of the Study

Within the modern paradigm of flattened organizational structures, end users are afforded a high degree of autonomy in terms of decision making. Their span of control may reach as far as interdepartmental issues relating to productivity, human resources, finance and intellectual capital or only as far as to encompass issues relating to their immediate tasks. It is safe to assume that regardless of the nature of the decision making responsibility, critical decisions regarding the effective and proper use of computing resources is a concern. Given the inherently hazardous climate within which most computing environments exist, it is no wonder that a prominent concern among the majority of the user community is that of effective computer security management.

The realm of computer security management offers a unique environment in which to apply a proven social influence technique because it is one in which its target audience (end users) engage in system activities to which they approach from various levels of proficiency, interest and vigilance. Often, regardless of the status of these qualities, they are expected to actively participate in decisions and actions concerning the

protection of their respective computing facilities. As such, end user attitudes and behavioral intentions are critical variables which must be understood and positively influenced.

To effectively influence end user attitudes and intentions concerning individual computer security management, high-level management personnel (CIO or CSO) must understand the issues surrounding the proper use of persuasive messages. Because fear appeals represent a significant portion of persuasive communications within the computer security domain, knowledge of how these messages affect change on an individual level is critical. Improper use of fear appeals may have unintended consequences that can jeopardize the integrity of the entire organization's computer infrastructure. Additionally, for those organizations seeking to utilize fear appeals to promote effective individual computer security management, knowledge of the role of source credibility is equally important.

Organization

This dissertation is comprised of five chapters and three appendices. The first chapter presents an overview of the utility of persuasive communications, concentrating on the practice and promise of fear appeals in the area of computer security management. Chapter One also provides an overview of acceptance models and source credibility. Acceptance models, in particular UTAUT, provide the theoretical foundation for this research, while source credibility is included in this study because of its considerable role in persuasive communication research. The objectives of the research, as well as an

overview of the proposed research model, the research methods, and significance of the study are also provided within the first chapter.

The second chapter concentrates on exploring the previous literature concerning the primary theories involved in the study: fear appeals, UTAUT, and source credibility. While devoted to the presentation of the theories of interest to this study, Chapter Two culminates in the formation of a research model and its related hypotheses.

The third chapter provides definitions of the constructs of interest and describes in detail the two-phase investigation involved in this study. Included in this discussion are details of the research methods, research instruments, and statistical techniques utilized in both the preliminary and primary investigation phase. The pilot study is also described in this chapter.

Chapter Four details the results of analysis involved in both the preliminary and primary phase of this investigation. Included in this discussion are results of the preliminary phase of investigation in which the experimental treatment and research instrument were subjected to tests of content validity, and the instrument was subjected to a construct validity test. The discussion of results from the primary phase of investigation include characteristics of the data sample, results of tests of internal and external validity based on the Solomon four-group research model, and tests of the conceptual model using Structured Equation Modeling (SEM). The chapter concludes with an interpretation of the results of the model testing in terms of supported and nonsupported hypotheses.

Finally, chapter five describes the implications of this research both to academia and to practice. The limitations of the study are described, as are directions for future research.

CHAPTER II

LITERATURE REVIEW

While the previous chapter served as an overview of this research, including an introduction to its theoretical underpinnings, conceptual model, objectives, research methods, and significance, this chapter provides a detailed review of the literature regarding the primary theories addressed in the study. Additionally, this chapter articulates the formulation of the conceptual model to explain and predict the influence of fear appeals on attitudes and intentions toward recommended individual computer security action. Furthermore, the relationships within the proposed model are posited as testable hypotheses.

Fear Appeals Defined

Simply put, a fear appeal is a persuasive message with the intent to motivate individuals to comply with a recommended course of action through the arousal of fear associated with a threat. “Fear appeals are persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends” (Witte, 1992, p. 329). The required elements of a fear appeal are inferences to the *severity* of a threat, the individual’s *susceptibility* to the threat, as well as statements of *efficacy* in terms of a recommended response and the ability of the individual to perform the recommended response.

Within the introduction of his chapter, “Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation,” Rogers (1983) revisits a Jonathan Edwards’ passage:

O Sinner! Consider the fearful danger you are in. It is a great furnace of wrath, a wide and bottomless pit, full of the fire of wrath ... The use of this awful sermon may be for awakening unconverted persons in the congregation. This that you have heard is the case of every one of you ... And now you have an extraordinary opportunity, a day wherein Christ has thrown the door of mercy wide open ... a day wherein many are flocking to him, and pressing into the kingdom of God. (p. 163)

Rogers claims that all of the elements of a fear appeal are present within this passage: (a) a claim of a severe threat in that the reader is in imminent danger of everlasting turmoil; (b) implication of relevance to the reader in that the message implicitly states that you, the reader, are the subject in peril; (c) a statement of efficacy in that many are choosing to take a “wide open” path; and (d) a recommended course of action in that the solution to the problem is to flock to Christ.

While this passage could be considered a classic example of a fear appeal, traditional applications of fear appeals are found in the areas of healthcare and marketing (LaTour & Rotfeld, 1997; LaTour & Snipes, 1996) in which the threat of physical harm or emotional trauma is offered as a consequence to an imminent threat. For example, anti-smoking advertisements have frequently used strong appeals to the fear of emphysema, lung cancer, or other health threats as consequences associated with

smoking. Studies conducted in this domain often seek to investigate the effect of fear appeals on attitude change by subjecting an individual to a persuasive message that articulates a potentially harmful consequence associated with a specific course of action (Rogers, 1983). What follows is a declaration of a reasonable and effective recommended course of action to ameliorate the threat, thereby avoiding the negative consequences.

Fear appeals, otherwise known as threat appeals or fear communications, can be defined either by the content of their message or by the response they command from their target audience (O'Keefe, 1990). For example, a fear appeal may use vivid or personalistic language to enhance the relevance of the message. In a study to investigate the persuasive impact of vivid information toward attitude change, Sherer and Rogers (1984) determined that emotionally interesting information, as well as concrete, specific information had a positive affect in changing attitudes.

In the context of fear appeals to modify attitudes or behavioral intentions to accept and use computer security technologies, vivid information may include depictions of personal financial ruin, as well as references of totality and ultimate disaster. Also, graphic depictions of disaster or peril are frequently included in the contents of a fear appeal. The graphical element has proven to be effective in inciting changes in attitude, behavioral intent, and behavior (Schneider et al., 2001).

Alternatively, the degree to which a message recipient experiences physiological or psychological arousal as a direct result of a fear appeal has been used in defining fear appeals. O'Keefe (1990) argues that the majority of fear appeal investigations involve

some form of testing for audience response. These studies involve fear-arousing statements which incorporate vivid, personalistic, or graphic imagery to purvey a sense of relevance and severity of consequences to the message recipient. In other words, a conventional definition of a strong fear response includes both the depiction of a severe threat by the message purveyor and the perception of a severe threat by the recipient.

In discussing the influence of fear appeals in modifying attitudes and behavioral intentions toward the use of computer security technologies, it is important to clearly define all elements of a fear appeal. The three main constructs in fear appeals are fear, threat, and efficacy (Witte, 1992).

Fear

Fear is defined as an internal emotional reaction composed of psychological and physiological dimensions that may be aroused when a serious and personally relevant threat is perceived (Witte, 1994). Cannon (1915) and Freud (1936) describe fear as a motivational state in response to impending danger. Lang (1984) describes fear as a negative valence emotion that is instantiated in memory as an associative network of stimulus, response, and meaning propositions. Stimulus propositions contain information about stimuli and the relevant context of their occurrence, while response propositions describe verbal behavior, overt acts, as well as physiological responses consistent with the context of the stimuli. The meaning propositions provide significance to any arousal generated by the stimuli as well as any action taken in response. The resultant data structure, also referred to as an emotion prototype, may be activated when propositions in the prototype are instigated by either actual or descriptive fear inducing objects such as

the presence of a snake or the descriptive narration of a relevant severe threat. The probability of activation is dependent upon many factors including the consistency, completeness, and form of stimulus information. While a natural language narrative of a threat such as a flash flood may access a fear prototype stored in long-term memory, the probability of prototype activation will increase as more propositions within the prototype are instigated. For example, the same natural language narrative of a flash flood will be more likely to activate a fear prototype if the experience occurs during a severe rain storm.

Fear is a primitive, natural emotional state to which no human being is immune (Ortony & Turner, 1990). While the causes of fear vary from one individual to another, the clues are either natural or cultural (Izard, 1977). Natural causes of fear include conditions such as isolationism, pain, abrupt changes in environment, as well as fear itself (Izard, 1977). Izard (1977) explains that many of the socio-cultural (learned) causes of fear are at least partially related to the innate causes. However, the probability of fear induced by these stimuli is unique to an individual and is moderated by individual characteristics grounded in biological differences and socialization experiences.

Fear response may be realized in the form of a verbal expression, an overt act such as a facial expression, or a physiological manifestation such as decreased skin temperature or an increased heart rate (Dillard, 1994). Both Izard (1977) and Dillard (1994) describe the facial expression of fear as comprised of slightly raised, clinched eyebrows such that horizontal wrinkles are present across part of the forehead. The eyelids are adjusted such that the upper eyelid is slightly raised while the lower eyelid is

tightened. Also, the corners of the mouth are horizontally stretched. However, from a measurement perspective, Mewborn and Rogers (1979) found that self-reported measures of fear are consistent, if not preferable, to physiological measures such as blood pressure and skin conductance. “The emotion of fear has been of interest because of its role in mediating attitude and behavior change” (Rogers, 1983, p. 155). In terms of fear appeal studies, fear is an emotional state that is derived from stimuli that seek to motivate changes in attitudes toward actions that would otherwise facilitate negative consequences. “Fear arousing stimuli seek to eliminate response patterns that produce aversive consequences (e.g., cigarette smoking) or establish response patterns that might prevent the occurrence of noxious events (e.g., taking prescribed inoculations)” (Rogers, 1983, p. 154).

Fear has been found to play an increasing role in the marketing of computer security software (Whaley, 2005). Whaley (2005) states that in a review of the promotional endeavors of the prominent information technology (IT) security firms, “most use scare tactics to sell their products” (p. 17). The prominent contention among these firms is that by describing undesirable consequences associated with malicious computing activity, the majority of computing professionals and end users will experience the emotion of fear. From this merchants hope that purchases are made.

Threat

As defined by Witte (1992), a threat is an external stimulus variable that exists whether or not it is perceived by an individual. If an individual perceives the threat, that individual can be described as having an awareness of a threat. A properly constructed

fear appeal not only serves to induce cognitions that a threat exists but also purveys the severity of the threat and its target population's susceptibility to the threat. From this message, an individual is able to formulate a perceived severity of the threat and a perceived susceptibility to the threat. In other words, once an individual is conscious of a threat, he or she will establish beliefs as to the seriousness of the threat and his or her probability of experiencing the threat.

Threats to computing facilities exist in many forms, from many sources, and under different intentions (Loch et al., 1992). Regardless of whether or not the target of an instantiated threat is aware of its existence, threats are prevalent and constantly evolving. Presently, considerable press has been given to the dangers and methods for amelioration of spyware. Spyware is a particularly devious form of malicious code that can invade an end user's computer and compromise not only the functionality of the resource but also the privacy of the user (Wildstrom, 2005). Additionally, these infections can occur with the consent of the operator or under stealth conditions. Therefore, for many unsuspecting end users, spyware represents a threat that is beyond their current realm of awareness.

Efficacy

A fear appeal will contain arguments that cause an individual to form cognitions about efficacy. This perception of efficacy includes cognitions of the efficacy of the recommended response and the efficacy of the individual in performing the response (Witte, 1994). The former is referred to as response efficacy and is the degree to which an individual believes the response to be effective in alleviating a threat; while the latter

is referred to as self-efficacy and is the degree to which an individual believes in his or her ability to enact the recommended response (Rogers, 1975, 1983; Witte, 1992).

Within the context of computer security management, purveyors of computer security software place an emphasis on the capabilities of their software, as well as the abilities of its users. For a fear appeal to be successful in this highly technical context, statements of encouragement must be available. These statements may address installation ease, procedure simplicity, or software functionality.

Fear Appeals Research Overview

Studies concerning the impact of fear-inducing communications have evolved from the early works of Janis and Feshbach (1953) in which fear appeal strength was correlated with teeth brushing recommendation compliance. This evolution is reflected in the models used to explain fear appeal effects, such as those which model a curvilinear relationship between fear appeal strength and attitude change (Janis, 1967; McGuire, 1968) as well as those which suggest a linear relationship (Rogers, 1975). Witte (1998) contends that these early works, in conjunction with the works of Leventhal (1970, 1971) provide a necessary progression from which contemporary research models are derived.

The majority of research on fear appeals was conducted prior to the emergence of dual process theories of attitude and behavioral change (Hoog, Stroebe, & Wit, 2005). As described by Hoog et al. (2005), this initial research was guided by reinforcement theory in which Hovland, Janis, and Kelly's (1953) fear-as-acquired drive model dominated. Leventhal's (1970, 1971) parallel process model set the stage for contemporary cognitive theories such as Roger's (1975, 1983) protection motivation

theory and Witte's (1992) extended parallel process model. Table 2.1 provides a listing of some of the most noteworthy works, including their significance and theoretical advancement.

Table 2.1 Fear Appeal Research, Significance and Theoretical Advancement

Research	Significance	Theoretical Advancement
Hovland, Janis & Kelly (1953)	investigated factors which determine the effectiveness of fear appeals	fear-as-acquired model (drive model)
Janis (1967)	described an inverted U-shaped relationship between fear and message acceptance	fear-as-acquired model (drive model)
McGuire (1968, 1969)	described a two factor (cues and fear) theory to explain an inverted U-shaped relationship between fear arousal and attitude change	fear-as-acquired model (drive model)
Leventhal (1970, 1971)	distinguished between cognitive and emotional appraisals of fear appeals	parallel process model
Rogers (1975, 1983)	specified perceived susceptibility, perceived severity, and response efficacy as components of a fear appeal	protection motivation theory
Maddux & Rogers (1983)	added a fourth component, self-efficacy to protection motivation theory	protection motivation theory
Witte (1992)	extended the parallel process model by describing cognitive and emotional model appraisals as sequential processes and established the role of fear as an indirect motivator of behavioral change	extended parallel process model

Primary Fear Appeal Theories and Models

Scholars suggest there are four primary theories and models that serve as underpinnings for the majority of research in this field (Roskos-Ewoldsen et al., 2004; Witte, 1992). The earliest is that of Hovland et al. (1953) and is referred to as the Fear-as-Acquired Drive Model. One of several competing models that are collectively described as drive models, this model was eventually supplanted by Leventhal's (1970, 1971) Parallel Process Model which was itself succeeded by Roger's (1975) Protection Motivation Theory. While these theories provide some explanation for how and why individuals react to fear appeals, each theory is deficient in some respect in providing an integrated explanation of the conditions under which fear appeals succeed and fail in affecting changes in attitude and behavioral intent (Witte, 1998). Witte's (1992) Extended Parallel Process Model (EPPM) seeks to fill that void by incorporate key components of the previous theories into a single model.

Drive Models

Early research on fear-inducing persuasive communications regarded fear as a negative emotional state that motivates an individual to take action to alleviate the negative emotional condition. A pioneering theory of fear and motivation, the Fear-as-Acquired Drive Model was first introduced by Hovland et al. (1953) and later modified by Janis (1967). This model described the relationship between motivation and fear as an inverted U-shaped relationship. Janis' contention was that some degree of fear arousal must be present in order to induce a motivation for behavior consistent with alleviating the threat (adaptive outcome). However, too much fear arousal would result in behavior

consistent with alleviating the fear (maladaptive outcome). Janis argued that the negative emotional state caused by fear drove individuals to take action to reduce their fear.

Furthermore, any action that decreased their fear, regardless of whether it was an adaptive response or a maladaptive response, would pacify their cause and become a preferred response.

A similar theory posited by McGuire (1968, 1969) also described an inverted U-shaped relationship between fear arousal and attitude change. In describing his two-factor theory, McGuire argued that individuals took actions consistent with the message's recommendation when fear acted as a drive. However, when fear acted as a cue, habitual responses to the fear inhibited the adoption of the recommended response.

These early drive models of fear appeals and attitude change, as established by Janis (1967) and McGuire (1968, 1969), have since been overwhelmingly rejected (Beck & Frankel, 1981; Rogers, 1983; Sutton, 1982). Ultimately, a direct relationship between drive and attitude change was never supported (Leventhal, 1970; Rogers, 1983) and arousal, not arousal reduction, was determined to influence behavioral intent (Mewborn & Rogers, 1979).

Parallel Process Model

Following extensive research toward the advancement of fear appeal theory, Leventhal (1970, 1971) proposed a Parallel Response Model that served to distinguish an emotional response to fear-inducing communications from a cognitive response (Rogers, 1983). Later referred to as the Parallel Process Model, Leventhal's model proposed that fear appeals may instigate either a process that serves to avert the danger (*danger control*

process) or a process that functions to alleviate fear (*fear control process*). Equally important to the differentiation of emotional and cognitive responses is the contention that the two processes are independent of each other. In other words, adaptive behavior is not influenced by fear but by cognitions intended to address the danger.

Leventhal's model was the first to distinguish between the type of response elicited by a fear appeal as being either emotional or adaptive. Leventhal (1970, 1971) argued that when an individual's emotions drive the response to a fear communication, that person then is engaging in a fear control process. Conversely, if the individual's cognitions of the threat dominate his or her response, then the person is engaging in a danger control process.

Fear control processes can be described as coping responses that are intended to reduce fear. These processes become dominant when individuals perceive a significant and relevant threat but do not perceive themselves as capable of performing a recommended response to alleviate threat or do not perceive the recommended response as sufficient to alleviate the threat. When fear control processes are dominant, individuals will engage in denial, defensive avoidance, and message derogation whereby their actions deviate from those prescribed in the message. Danger control processes can be described as protection motivation responses that are intended to avert a significant and relevant perceived threat. These processes become dominant when individuals perceive themselves to be susceptible to a severe threat and also capable of averting the threat. When danger control processes are dominant, individuals will demonstrate positive attitudes, intentions and behavior toward adopting a recommended response.

In summary, the Parallel Process Model provides that fear appeals generate persuasion and fear and that fear does not cause persuasion. When presented with a fear-inducing message, individuals will either respond with processes aimed at reducing the threat or with processes designed to reduce their fear. This model also suggests that whatever the response, the individual will use this experience to shape his or her subsequent responses to future fear arousing communications.

Protection Motivation Theory

Building on Leventhal's (1970, 1971) Parallel Process Model, Rogers (1975) concentrated on expounding on the processes involved in coping with a threat. He argued that there were three primary components of a fear appeal that attributed to the manner in which its audience would respond. The components were identified as perceived susceptibility, perceived severity, and response efficacy. The later work of Maddux and Rogers (1983) resulted in the addition of a fourth component, self-efficacy. It was Rogers' contention that when each of these components were at high levels, an individual's protection motivation would also be at a high level, thereby increasing the probability of change in his or her attitude and behavioral intent.

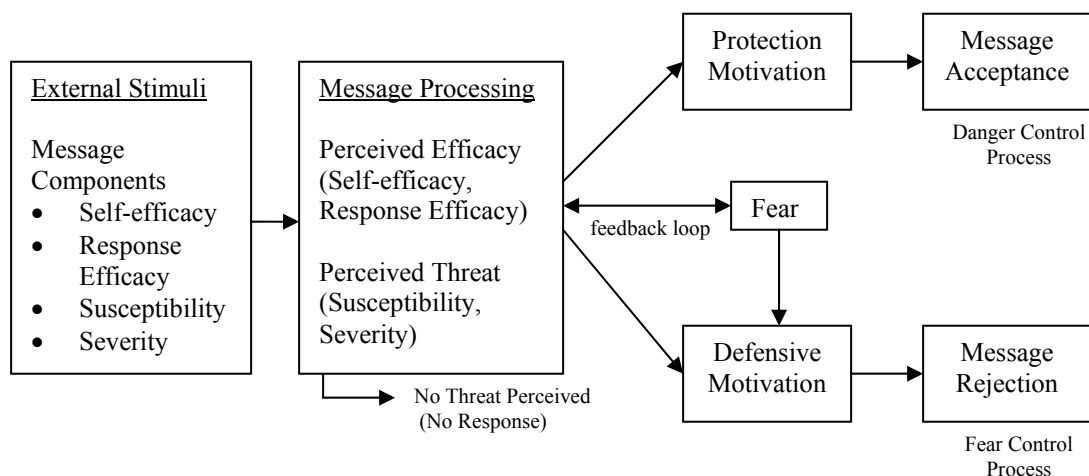
Any change in attitude and behavioral intent was regarded by Rogers (1983) as a response to the fear appeal; however, Rogers acknowledged that a response may be either adaptive or maladaptive. The Protection Motivation Theory suggests that when an individual believes a recommended response to a threat is feasible and effective, and that performing the response is of greater value than any costs associated with that response, he or she will be inclined to perform the recommended response. This type of response,

toward amelioration of a threat, is referred to as an adaptive response. Conversely, if an individual believes the benefits associated with not following a recommended response to be greater than the value found in performing the response, he or she is more likely not to perform the recommended action. This type of outcome is referred to by Rogers (1983) as a maladaptive response.

A review of the literature finds the Protection Motivation Theory applied within a large number of studies, mostly concentrated within the healthcare domain. For instance, in a study involving African American youth, Wu et al. (2005), applied the protection motivation theory to assess health protection motivation regarding drug trafficking intervention initiatives. Protection motivation theory was also applied by Grunfeld (2004) to examine college students' intentions to practice safe sun exposure activities, as well as Cates, Dian, and Schnepf (2003) to assess the fear of crime in rural areas. Clearly, the Protection Motivation Theory maintains a significant position among theories designed to predict and explain an individual's reaction to a fear-inducing communication.

Extended Parallel Process Model

Witte (1992) examined the existent models concerning fear appeals and concluded that a gap existed in describing interactions of the components of a fear appeal as well as the role of fear itself in persuasive arguments. What followed was a theoretical combination of Leventhal's (1970) Parallel Process Model and Rogers' (1983) Protection Motivation Theory that serves to more accurately explain how fear appeals influence or do not influence the behaviors of its audience (see Figure 2.1).



Source: Witte, K. (1998) Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Process Model to Explain Fear Appeal Successes and Failures. In P. A. Andersen & L. K. Guerrero (Eds.), *Handbook of Communication and Emotion: Research, Theory, Applications, and Contexts* (pp. 423-450). San Diego, CA: Academic Press.

Figure 2.1

Extended Parallel Process Model

According to Witte (1992), a fear appeal consists of two parts. The first part contains statements designed to increase perceived threat by articulating the severity of a threat (i.e., the degree of harm associated with a threat) and the probability of the threat occurring. The second part attempts to enhance the perceived efficacy associated with a recommended response by (a) providing unambiguous and feasible steps to avert the threat and (b) highlighting the value of the recommended response in averting the threat (McKay, Berkowitz, Blumberg, & Goldberg, 2004).

The Extended Parallel Process Model (EPPM) posits that fear appeals instigate two sequential appraisals consistent with the structure of the message (Witte, 1992). The

first appraisal is with regard to the threat, while the second appraisal addresses the efficacy of the recommended threat response. Only if a threat is perceived to be relevant and potentially harmful will an appraisal of efficacy occur. In other words, if an individual is exposed to a fear appeal that does not arouse a personally relevant perception of threat, then no further information processing occurs.

As described above, both the threat and efficacy constructs consist of two dimensions. When an individual appraises a threat, that individual will consider his or her susceptibility to the threat as well as the severity of the threat. The resultant perceived threat represents the individual's cognitions about the identified threat articulated in a fear appeal. Pertaining to the effectiveness, feasibility, and ease with which a recommended response ameliorates a specific threat, efficacy appraisal also involves the consideration of two dimensions, response efficacy and self-efficacy. Response efficacy represents the degree to which the individual believes the response to be effective in impeding a threat. Self-efficacy refers to the degree to which the individual believes he or she is capable of performing the recommended response to the threat. Together, response efficacy and self-efficacy represent a perceived efficacy that will ultimately determine the manner in which the individual will react to the threat.

In circumstances where a fear appeal was successful in eliciting a significant perception of threat, an evaluation of the efficacy of the response and self follows. As described by EPPM, individuals with a heightened threat perception in conjunction with a high degree of perceived efficacy will take action to ameliorate the threat. This type of behavior is described as a danger control process, which is a cognitive process whereby

strategies are employed to avert a threat. However, in situations in which perceived efficacy is less than perceived threat, individuals will engage in actions to suppress their fear rather than manage the threat. This type of behavior is described as a fear control process whereby individuals will employ coping responses to diminish fear.

EPPM establishes fear as an indirect motivator for behavioral change. Fear is an emotion associated with a threat, whether perceived or real, that is an unintended consequence of a computing environment. The primary motivation in accepting and engaging in computer security activities is to avoid negative outcomes associated with a threat. From this perspective, fear is an emotional antecedent associated with acts that are not intended to generate performance or satisfaction gains. Instead, computer security acceptance and use behaviors are intended to defuse existing negative performance or prevent undesirable consequences inherent in modern, interconnected computing environments.

Fear/Threat Relationship

EPPM maintains that when individuals engage in fear control processes, the outcome is message rejection. In this state, cognitions of the threat and efficacy of the recommended response are absent and the emotion fear is prominent. Alternatively, when individuals perceive an effective and feasible response to avert a threat is available, only thoughts of the threat and efficacy will directly influence message acceptance. It is in this state however, that EPPM suggests that the emotion fear is cognitively appraised and can actually lead to changes in the level of perceived threat. In other words, persons with a high perception of efficacy may notice physiological symptoms associated with

fear, such as sweating palms or a racing pulse, and consider these symptoms to mean that they perceive the threat to be greater than they originally thought. From this upgrade to perceived threat, their motivation for message acceptance is positively adjusted.

The outcome of interest in fear appeal research is often message acceptance. EPPM provides one theoretical model to explain message acceptance. The fields of psychology and social science provide other models that explain and predict acceptance. Within the field of IS, a significant amount of interest is in the area of technology acceptance. The following section presents a review of the prominent acceptance models leading up to and including the Unified Theory of Acceptance and Use of Technology (UTAUT).

Acceptance Models

User acceptance of a technology has been recognized as a critical determinant of success in attempts to establish new information systems (IS) within an organization (Al-Gahtani & King, 1999; Davis, 1993; Davis et al., 1989; Igarria & Chakrabarti, 1990; Swanson, 1988; Thompson, Higgins, & Howell, 1991). Additionally, previous research has established the importance of understanding the antecedents of a person's attitudes, intentions, and behavior within the context of IS (Al-Gahtani & King, 1999; Delone & McLean, 1992; Etezadi-Amoli & Farhoomand, 1996; Igarria, 1990; Igarria & Chakrabarti, 1990; Lee, 1986; Robey, 1979; Swanson, 1982; Torkzadeh & Dwyer, 1994). Rooted in several distinct disciplines, there are numerous theories that serve to guide research purposed toward the acceptance and use of technology. Within the context of this research, however, the specific interest in behavioral intentions toward recommended

IT security related actions dictate the detailed investigation of those theories leading up to and including UTAUT, the most comprehensive model purposed toward this goal.

Based on eight competing models found in the psychological, social and behavioral sciences, UTAUT represents a parsimonious synthesis of the models' most significant factors. The eight models, in no particular order, are as follows: (a) Theory of Reasoned Action (TRA); (b) Technology Acceptance Model (TAM); (c) Theory of Planned Behavior (TPB); (d); Combined TPB and TAM (C-TPB-TAM); (e) Motivational Model (MM); (f) Model of PC Utilization; (g) Social Cognitive Theory (SCT); and (h) Innovation Diffusion Theory (IDT). Within the field of IS, the majority of studies concerning technology acceptance have been guided by the TAM. For this reason, overviews of the eight models synthesized to form UTUAT are provided, with particular emphasis placed on TAM.

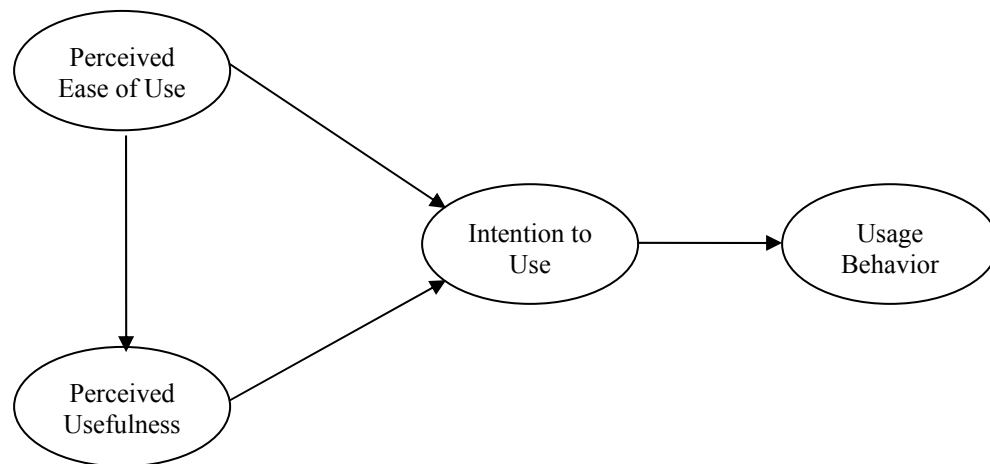
The Theory of Reasoned Action (TRA), first described by Fishbein and Ajzen (1975), provides a simple yet effective model for predicting behavioral intent and behavior. This theory dictates that individuals' attitudes and subjective norms influence their behavioral intent and subsequently their behavior. Although initially posited in the context of consumer behavior, particularly voluntary behavior, the model has been applied beyond its intended domain and conditions with positive results (Sheppard, Hartwick, & Warshaw, 1988). Interestingly, TRA was used in a study of the impact of persuasive messages on attitudes and subjective norms with not such positive results (Lindsey, 2004). In this study, 276 undergraduate students were randomly assigned to three groups and exposed to persuasive messages intended to modify either attitudes or

social norms (the third group was a control group) concerning eating habits. The results of the study indicated that TRA was unable to predict student behavior.

TAM (Figure 2.2) has served as a theoretical foundation for numerous studies which seek to explain individual behavioral intentions within fields ranging from online shopping experiences (Shang, Chen, & Shen, 2005) to law enforcement (Colvin & Goh, 2005). For instance, Keat and Mohan (2004) used TAM as the foundation for their study of the acceptance of electronic commerce by Internet users and the development of a synthesized model of electronic commerce based TAM models. According to the Institute for Scientific Information's Social Science Citation Index, since 1999, 531 published research works cite Davis' (1989) original MIS Quarterly manuscript. TAM's strength lies in its parsimony and its purpose in an age of technological evolution. While numerous studies have added constructs to the TAM in an attempt to increase its predictive power, the simplistic nature of the model has endured.

TAM predicts the acceptance and use of information technology (Davis, 1989) and establishes perceived usefulness and perceived ease of use as predictors of behavioral intention specifically within the context of information technologies (Figure 2.2). Originally included in studies of system utilization by Schultz and Slevin (1975), perceived usefulness is described in TAM as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p. 320). Robey (1979) eloquently articulated the importance of perceived usefulness by noting that if a system does not provide utility to those who use it, then it will simply go unused. Perceived ease of use is described as "the degree to which a person believes that

using a particular system would be free of effort” (Davis, 1989, p. 320). The original investigation of the role of perceived ease of use is found in Bandura’s (1982) work involving a similar latent variable, self-efficacy. Bandura found that expectations of one’s ability to execute actions necessary to cope with a particular situation influence that person’s actual behavior.



Source: Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 318-340.

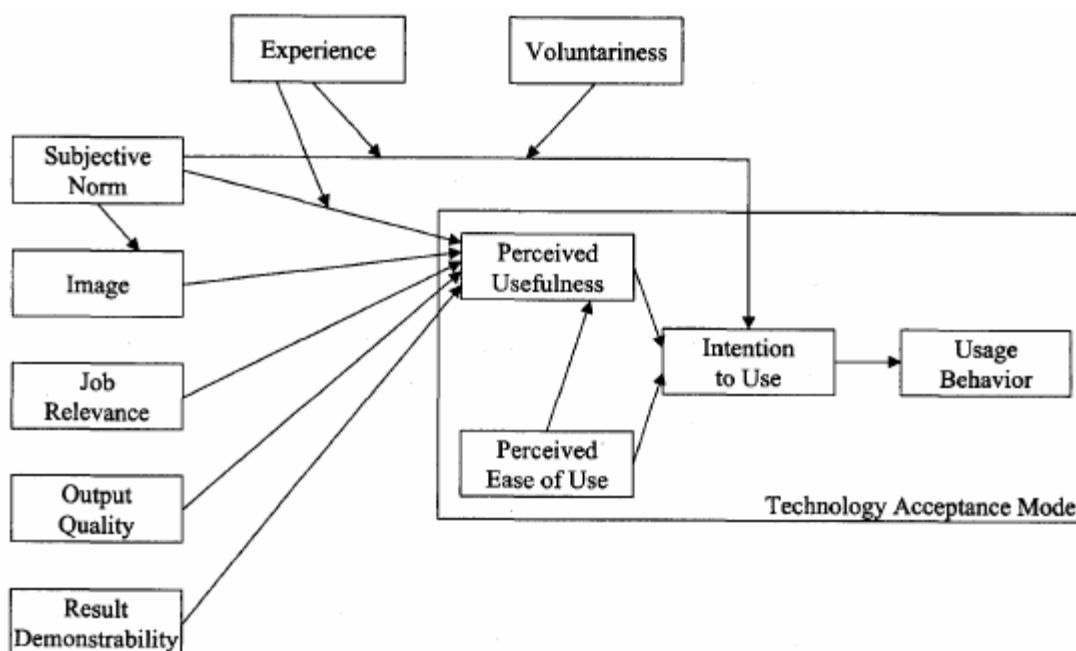
Figure 2.2

Technology Acceptance Model (TAM)

TAM originally included attitude toward use as a determinant of usage behavior. Borrowed from Fishbein and Ajzen’s (1975) Theory of Reasoned Action (TRA), attitude was ultimately dropped by Davis (1989) in an effort to streamline the model as much as possible. TRA was instrumental in the development of TAM and, when applied by Davis et al. (1989) to explain the individual acceptance of technology, was found to be well suited to the study of behaviors involving technology.

Empirical tests of TAM have consistently found it to explain about 40% of the variance in usage intentions and use behavior (Davis, 1989). Recent studies have extended TAM and have encountered encouraging results. For example, through the incorporation of Internet self-efficacy into TAM, Ma and Liu (2005) found that 80% of the variance in behavioral intent toward the acceptance of web-based electronic medical records was explained.

Venkatesh and Davis (2000) extended TAM to what they refer to as TAM2 by integrating both social influence processes and cognitive instrumental processes into the model (Figure 2.3). Through the incorporation of subjective norm, image, job relevance, output quality, and result demonstrability, TAM2 is able to account for up to 60% of the variance in perceived usefulness, a driver of usage intent (Venkatesh & Davis, 2000). Within a mandatory setting, subjective norm was found to exhibit a more profound affect on usage intentions than perceived usefulness and perceived ease of use. First explored by Fishbein and Ajzen (1975) within TRA, subjective norm refers to an individual's perception that the majority of people of importance to him or her support a particular behavior in question. However, the effect of subjective norm was found to degrade over time as end users became more experienced with the technology (Venkatesh & Davis, 2000).



Source: Venkatesh, V., & Davis, F.D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 46(2), 186-204.

Figure 2.3

TAM2

Building on the strong foundation provided by TRA, the Theory of Planned Behavior (TPB) modified TRA by including perceived behavioral control in the model. Within the context of IS, several studies have successfully applied TPB to predict individual acceptance and use of technology. For instance Harrison et al. (1997) utilized TPB to explain and predict the decisions made by executives concerning the acceptance of technology within small business. Subsequent research along this line resulted in a Combined Model of TPB and TAM (C-TPB-TAM). This combined model provided for improved explainability over TAM or TPB alone regarding small business executive

decisions concerning web technology (Riemenschneider, Harrison, & Mykytyn, 2003). More importantly, it represented a fusion of theories deriving from the initial models of TRA and TAM.

Also within this time frame, additional theories grounded in psychology and human behavior were posited. The Motivational Model (MM) established extrinsic and intrinsic motivation as determinants of an individual's behavior. Within the context of IS, Davis et al. (1992) applied MM to help explain behavioral intent toward computer use in the workplace. Additionally, Venkatesh and Speier (1999) were able to determine that an individual's intrinsic motivation toward the use of a new technology could be affected by his or her mood during training exercises. Following the work of Trandis (1977) in human behavior, Thompson et al. (1991) examined responses from knowledge workers within a multinational organization to determine the factors that were significant in determining the degree to which personal computers were utilized. Their findings supported the constructs of job-fit, complexity, long-term consequences, affect toward use, social factors, and facilitating conditions as determinants of behavior and became known as the Model of PC Utilization (MPCU).

Based on the works of Bandura (1986), Compeau and Higgins (1995a, 1995b; Compeau, Higgins, & Huff, 1999) were the first to apply the Social Cognitive Theory (SCT) within the domain of IS acceptance. In examining an individual's affective and behavioral reactions to IT, the authors found significant relationships between these outcomes, self-efficacy, performance expectations, and personal expectations (Compeau & Higgins, 1995b). Grounded in Roger's studies within the field of sociology, the

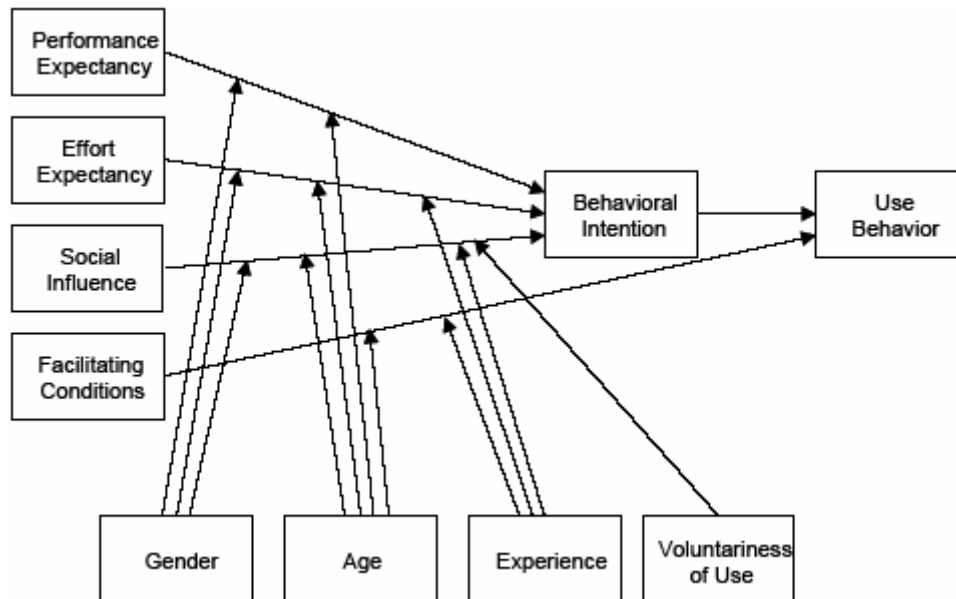
Innovation Diffusion Theory (IDT) has proven to be a useful theory for the study of an individual's perceptions regarding the adoption of IT. Moore and Benbasat's (1991) work involving IDT within the context of IS acceptance established relative advantage, ease of use, image, visibility, compatibility, result demonstrability, and voluntariness of use as key determinants of initial adoption and subsequent diffusion of IT within an organization.

Building on the findings of TAM and TAM2, and incorporating the most prominent theories of acceptance, behavioral intent and behavior, Venkatesh et al. (2003) developed UTAUT (Figure 2.4). Similar to their earlier acceptance models, this model provides explanatory ability for behavioral intent and behavior toward a new technology. Furthermore, UTAUT has been proven to predict approximately 70% of the variance in an individual's intentions and behavior toward the acceptance and use of a new technology. Because of its predictive ability, UTAUT has become the latest "model of choice" for studies involving technology acceptance and use.

The constructs included in UTAUT are performance expectancy, effort expectancy, social influence, facilitating conditions, behavioral intention, and use behavior. As indicated by the model, behavioral intention is directly determined by performance expectancy, effort expectancy, and social influence. Facilitating conditions and behavioral intention directly determine use behavior. Also depicted in the model are the relationship moderators, gender, age, experience, and voluntariness of use. These constructs and their reflective indicators are based on the empirical results of a longitudinal test of 215 respondents from four organizations. The constructs' indicators

are the four highest loading items for each construct borrowed from earlier models.

UTAUT was cross-validated using new data obtained from two additional organizations.



Source: 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.

Figure 2.4

Unified Theory of Acceptance and Use of Technology (UTAUT)

Not all of the latent variables of UTAUT were applicable to the proposed model. Descriptions of the omitted constructs, as well as the rationale for noninclusion are discussed next. For those constructs included in the model, their descriptions will be included in the section regarding research model and hypotheses development.

In forming their intentions to accept and use new technology, individuals will consider the amount of effort necessary to learn and apply the technology (Venkatesh et

al. 2003; Gefen, 2000). It can be expected that when individuals perceive a great amount of effort is required to understand and use a particular technology, they will be less inclined to adopt it. Venkatesh et al. (2003) determined that the relationship between effort expectancy and behavioral intentions is moderated by gender, age, and experience.

Effort expectancy was derived from a synthesis of both Davis' (1989) and Moore and Benbasat's (1991) definitions and items describing perceived ease of use, as well as Thompson et al.'s (1991) complexity construct. A close examination of the resultant items reveals similarities with the self-efficacy construct as developed by Bandura (1986) and operationalized in Witte et al.'s (1996) scale. Therefore, it is expected that if effort expectancy were to be included in the research model, then validity tests between constructs would not establish discriminant validity. For this reason, effort expectancy is not included in the research model.

Facilitating conditions refer to the degree to which an individual believes the organization supports his or her use of a technology (Venkatesh et al., 2003). For this study the definition is restated as the degree to which a user believes there exists favorable support for the application of anti-spyware actions. The support may come from a helpdesk, systems support personnel, vendor phone support or some other form of potential assistance to a user. It is reasoned that as the support options improve, the confidence a user has toward engaging in the recommended security action will also increase. However, Venkatesh et al. (2003) determined facilitating conditions to be a direct determinant of usage behavior, which is not a part of this study. Therefore,

facilitating conditions will not appear in the model, but remain significant for future research involving behavioral measurement.

Volunteeriness of use was also excluded from this model as it is only reasonable to assume that a fear appeal is only effective if the conditions are such that the user may consider his or her options for addressing threatening circumstances. UTAUT positions volunteeriness of use as a moderating variable for the relationship between social influence and behavioral intentions. However, in situations where the end user is mandated to follow a prescribed course of action to avert or reduce a threat, appraisals of efficacy and threat are not warranted.

Source Credibility

One of five components that McGuire (1978) identifies as part of persuasive communications, message source has been the focus of numerous studies among a wide variety of disciplines (Pornpitakpan, 2004). Source credibility has been the specific variable of interest among a many number of these studies and has involved many different dimensions such as expertise and trustworthiness (Berlo & Lemert, 1961; Hovland et al., 1953; O'Keefe, 1990; Pornpitakpan, 2004), physical attractiveness (Chaiken, 1979; Eagly & Chaiken, 1975), gender (Kenton, 1989), competency (Berlo & Lemert, 1961) and dynamism (Berlo & Lemert, 1961; Hewgill & Miller, 1965).

One scale, the McCroskey and Jenson (1975) Source Credibility Scale, includes 25 items to conceptualize the dimensions of competency, character, sociability, composure, and extraversion. A competing scale, the Leathers Personal Credibility Scale (Leathers, 1992), utilizes 12 items to conceptualize the dimensions of competence,

trustworthiness, and dynamism. It is worth noting that factor analytic tests of both the McCroskey and Jenson Source Credibility Scale and the Leathers Personal Credibility Scale provided evidence that the construct could be described using fewer dimensions (Powell & Wanzenried, 1995). In fact, empirical evidence indicates the possibility of a two-dimension solution for the measurement of source credibility (Powell & Wanzenried, 1995).

For purposes of economy and consistent with Berlo and Lamert's (1961) assertion of contemporary social science research practices, this research utilized the Leathers Personal Credibility Scale (Leathers, 1992). As previously described, this scale measures source credibility via the three dimensions of competence, trustworthiness, and dynamism. Competence refers to the degree to which a communicator is perceived as competent of producing correct assertions, while trustworthiness refers to the degree to which a message recipient perceives those assertions as being valid (Hovland et al., 1953). Dynamism refers to the degree to which a message recipient "admires and identifies with the source's attractiveness, power or forcefulness, and energy" (Larson, 1992, p. 226).

The prominent contention among scholars regarding source credibility is that a highly credible source will more effectively persuade an audience than a low credibility source (Horai, Naccari, & Fatoullah, 1974; Hovland & Weiss, 1951; Johnson & Izzett, 1969; Johnson, Torvicia, & Poprick, 1968; Kelman & Hovland, 1953; Lirtzman & Shuv-Ami, 1986; Maddux & Rogers, 1980; Miller & Baseheart, 1969; Powell, 1965; Ross, 1973; Schulman & Worrall, 1970; Warren, 1969; Watts & McGuire, 1964; Wittaker &

Meade, 1968). When approached within the framework of this study, credible sources have been found to be more effective than noncredible sources in inducing favorable attitudes (Mugny, Tafani, Falomir, Juan, & Layat, 2000) and behavioral compliance (Crano, 1970; Crisci & Kassinove, 1973; Gangloff, 1981; Levine, Moss, Ramsey, & Fleishman, 1978; Ross, 1973; Tybout, 1978). Specifically, the perceived credibility of the source has been determined to be positively correlated with a message recipient's intentions to accept and apply recommendations as posited by the communicator (Bannister, 1986; Suzuki, 1978).

Research Model and Hypotheses Development

Based on the literature of fear appeal theory (EPPM), acceptance theory (UTAUT), and source credibility, this study proposes a research model as a means of explaining user attitudes and behavioral intentions toward recommended individual computer security actions as advocated in persuasive communications. As shown in Figure 1.3 and replicated in Figure 2.5, the model is an adaptation of UTAUT which provides explanatory ability for behavioral intent and behavior toward the acceptance and use of new technology. The model is adapted by the addition of Witte's (1992) EPPM which provides explanatory ability for attitudes toward a recommended response in light of perceived threat severity, threat susceptibility, response efficacy and self-efficacy. Additionally, source credibility is included in the model to account for any possible influence message source may have on perceptions of threat severity and threat susceptibility.

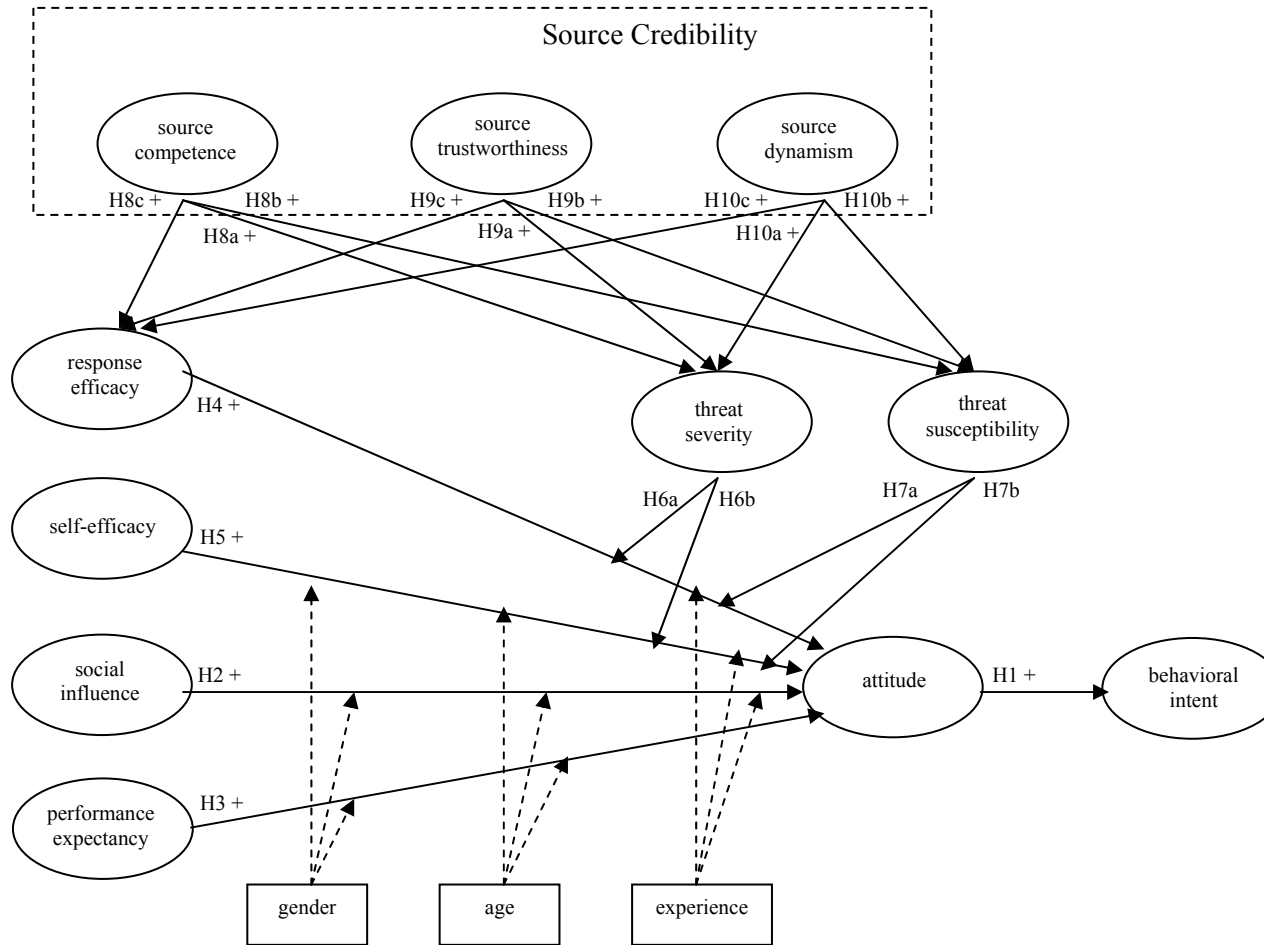


Figure 2.5
Conceptual Research Model

Although not depicted in the model, anxiety, affect, and affect toward use are constructs borrowed from Social Psychology theories for the investigation of their role in the prediction of behavioral intention in UTAUT. None of these constructs was found to have a significant influence on behavioral intention, thus justifying their absence from UTAUT as well as the current research model. However, these constructs do describe emotions associated by an individual with using a system. For example, joy, sadness, frustration, depression, disgust, and elation are feelings that an individual might have toward a particular act. Fear is another emotion that humans encounter and is associated with threatening conditions. Threats to secure computing are considered to be a reason for fear.

In its original form, UTAUT provides a validated model for explaining and predicting behavioral intentions toward IT. However, the circumstances surrounding the acceptance and use of computer security technology typically involve a perception of threat to the IT. The perception of threat is indirectly influenced by fear and can be explicitly addressed through fear-arousing messages. Considering the impetus for this study is to explore the influence of fear appeals on attitudes and behavioral intentions associated with individual computer security actions, the emotional aspects of acceptance and use behavior must be reconsidered and UTAUT should be modified accordingly.

Outcomes of the Model

The outcomes of the model are attitude and behavioral intent. Measurements of attitude and behavioral intent are not uncommon to IS research (Davis, 1989; Venkatesh et al., 2003). The preponderance of this research positions attitude as an antecedent of

behavioral intent, and behavioral intent as an antecedent of behavior. However, for the purposes of this study, behavior is not explored.

Attitude

Ajzen (1988) defined attitude as the inclination an individual possesses to react positively or negatively toward some element within his or her domain. Prior research contends that attitudes are based on cognitive evaluations of the positives and negatives associated with the element of interest (Ajzen, 1988). Within the context of IS management, these elements may be realized in the form of computer technology, implementation practices or persons of influence (Melone, 1990).

Previous research has demonstrated that an individual's attitude can have a significant impact on his or her computer usage behavior (Al-Gahtani & King, 1999; Fishbein & Ajzen, 1975; Igarria, 1990; Igarria & Chakrabarti, 1990; Robey, 1979). In fact, in tests of TRA, TPB, and MM, attitude was found to be the strongest predictor of behavioral intent (Venkatesh et al., 2003). Davis (1989) originally included attitude as a significant factor in predicting IS usage; however, further investigation (Davis et al., 1989) revealed attitude became barely significant when perceived usefulness was considered as a predictive variable. Ultimately, attitude was disregarded as having any significant predictive power and dropped from TAM and subsequent technology acceptance models (Davis, 1989; Davis et al., 1989; Venkatesh et al., 2003; Yang & Yoo, 2004). However, the rationale for exclusion from UTAUT was based on the presence of other key determinants. Venkatesh et al. (2003) reasoned that attitude was insignificant as a determinant of behavioral intention if included in the same model with effort

expectancy *and* performance expectancy. However, as explained previously, effort expectancy is excluded from the proposed model.

Interestingly, Yang and Yoo (2004) contend that Davis' (1989) studies failed to consider the cognitive aspect of the attitude construct, focused primarily on affective attitude and, in failing to do so, were limited in their ability to adequately test attitude's influence on behavioral intent. In fact, Goodhue (1988) argues that most IS research involving attitude fails to differentiate between its cognitive and affective dimensions. Based on social-psychological theories concerning attitude, Yang and Yoo divided attitude into its cognitive and affective dimensions and determined that cognitive attitude is a strong determinant of IS use.

The work of Yang and Yoo (2004) is especially interesting when juxtaposed with fear appeal theory. EPPM describes attitude as an outcome variable dependent upon cognitions of efficacy and suggests that these cognitions are moderated by perceptions of threat. In other words, cognitive appraisals of efficacy determine the nature of the attitude an individual assumes with regard to whether or not to follow a recommended response to a communicated threat, while perceptions of threat determine the intensity of the individual's attitude. Based on this knowledge and the findings of Yang and Yoo (2004), this study positions attitude as a significant factor in predicting a user's intentions to adopt or reject an advocated action. As such, the following hypothesis is offered:

H1: Attitude will have a significant positive effect on an end user's intent to adopt recommended individual computer security actions to ameliorate spyware.

Determinants of Attitude

Venkatesh et al. (2003) determined that one significant determinant of an individual's willingness to accept and use a new technology is the degree to which the individual perceives his or her friends, relatives, colleagues, and others whose opinions matter, support its acceptance and use. This determinant is referred to as *social influence* and is derived from a synthesis of three previously defined constructs within the technology acceptance literature (Venkatesh et al., 2003).

Social influence closely resembles social norm which was determined to be a significant determinant of attitude in the Theory of Reasoned Action (Fishbein & Ajzen, 1975), and the Theory of Planned Behavior (Ajzen, 1991). In those theories, it was determined that a person's attitude was influenced by the degree to which influential people support or admonish the outcome of a behavior (Venkatesh et al., 2003). Also, social influence relates to Thompson et al.'s (1991) construct of social factors which refers to an "individual's internalization of the reference group's subjective culture, and specific interpersonal agreements that the individual has made with others, in specific social situations" (Venkatesh et al., 2003, p. 452). Finally, social influence is closely related to Moore and Benbasat's (1991) construct image, which refers to the degree to which the use of an innovation is perceived to bolster one's social standing within his or her peer group.

It is expected that computer users will engage in discussions concerning the appropriate actions to take toward the security of their communications. One example could be found in the adoption of stringent password controls by end users based on

recommendations provided to them by colleagues or peers. Considering the added effort necessary to frequently change passwords in addition to the mental burden required to memorize complicated password schemes, a certain amount of social influence must be present in order for the end users to conform. It is expected that those responsible for security within an organization will frequently provide guidance and warnings to the users within the organization as to how to securely operate their computing resources. This form of social influence is provided electronically and face-to-face. It is with this understanding that the following hypothesis is offered:

H2: Social influence will have a significant positive effect on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware.

Performance expectancy can be described as “the degree to which an individual believes that using the system will help him or her better attain significant rewards” (Venkatesh et al., 2003, p. 447). This construct derives from the other constructs relating to performance expectancy that were established in several of the various models that were synthesized to form UTAUT. Perceived usefulness (Davis, 1989; Davis et al., 1989), extrinsic motivation (Davis et al., 1992), job-fit (Thompson et al., 1991), relative advantage (Moore & Benbasat, 1991), and outcome expectations (Compeau & Higgins, 1995b; Compeau et al., 1999) all describe a perception an individual holds of the relative advantage a system can provide toward the successful completion of his or her tasks (Venkatesh et al., 2003). Performance expectancy has been proven to be a strong predictor of attitude in previous tests (Witte, 1994), and this relationship is moderated by age and gender.

Within the context of computer security, it is important to articulate the distinct purpose of computer security action in terms of expected value. Computer security and information assurance, in general, are not intended to produce direct productivity gains. In fact, assurance mechanisms are intended to add complexity to a production environment. For instance, Warkentin et al. (2004) describe password mechanisms as devices with the purpose of complicating access to protected resources. As such, the use of them is not intended to provide productivity gains. Rather, password mechanisms are regarded as effective if complex enough to deter illegitimate access, while still allowing access for legitimate purposes. However, computer security actions do provide assurance from threats that can indirectly influence outcome expectations. Consider, for example, an end user that acquires, installs, and maintains anti-spyware software because it was advocated by the IT professionals within his or her organization. The protection afforded to the end user's data by the software increases the accuracy and consistency of the outcomes of his or her tasks. This assurance translates into enhanced quality and effectiveness in output. Therefore, it is hypothesized:

H3: Performance expectancy will have a significant positive effect on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware.

Within the proposed model, the two dimensions of perceived efficacy - response efficacy and self-efficacy - are positioned to act as direct determinants of attitude. As described earlier, response efficacy refers to the degree to which an individual believes a recommended response will effectively avert a threat (Rogers, 1975; Witte, 1992). For

the purposes of this study, response efficacy is considered within the context of individual computer security actions to impede or avert spyware.

Appraisals of response efficacy are considered to be a cognitive process whereby individuals form thoughts as to the effectiveness of a recommended response's ability to avert a threat (Witte, 1992). Ultimately it is their cognitions of response efficacy that will determine the manner in which they choose to address the threat (Witte, 1992).

According to Witte's (1992) EPPM, low levels of perceived response efficacy may lead to fear control processes whereby an individual will seek to reduce his or her fear.

Alternatively, high levels of response efficacy are associated with positive inclinations of threat amelioration whereby a recommended response is enacted. Consider an end user's contemplation of whether or not he or she will adopt a recommendation to protect against spyware through the installation and use of anti-spyware software. He or she will consider the capabilities of the software and form a disposition toward the recommendation based on this appraisal. It is with this understanding that the following hypothesis is offered:

H4: Response efficacy will have a significant positive effect on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware.

Similar to the manner in which an individual cognitively assesses the efficacy of a response, he or she also appraises his or her own abilities to perform the recommendation (Maddux & Rogers, 1983; Witte, 1992). First established by Maddux and Rogers (1983) as an extension to the Protection Motivation Theory and later incorporated into Witte's (1992) EPPM, self-efficacy is regarded as a determinant of attitude concerning a

recommendation to address a threat. Consider an end user's decision of whether or not to enact a recommendation to avert spyware intrusions. Even if he or she believes the advocated response to be effective, the end user must still consider his or her ability to successfully install and run the anti-spyware solution. From this insight, the following hypothesis is offered:

H5: Self-efficacy will have a significant positive effect on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware.

Moderating Effect of Perceived Threat

High levels of emotional arousal are considered to have a negative impact on self-efficacy (Kavanagh & Bower, 1985; Lazarus & Folkman, 1984; Marakas, Yi, & Johnson, 1998). Marakas et al. (1998) state that high levels of emotional arousal, such as that introduced by a perceived threat to the security of their digital assets, cause individuals to reduce their perceived capability to use a computer. Further, Gutek and Winter (1990) argued that high levels of emotional arousal are associated with degraded computer performance.

Threat Severity

As discussed earlier, perceived threat severity was first identified by Rogers (1975) as a primary component of a fear appeal that contributes to an audience's reaction. Perceived threat severity refers to the beliefs a fear appeal's audience has toward the significance of the threat (Rogers, 1975; Witte, 1992). EPPM establishes perceptions of threat severity as having the ability to moderate the intensity of the response as

established by perceptions of both response efficacy and self-efficacy (Witte 1992). For example, as an end user's perception of the severity of a spyware threat increases, his or her beliefs regarding the capabilities of anti-spyware software to adequately address the threat suffer. Additionally, fluctuations in the perceived severity of the spyware threat cause the end user to reassess his or her ability to successfully enact anti-spyware protection. From this argument, the following hypotheses are offered:

- H6a: The influence of response efficacy on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware will be moderated by his or her perception of threat severity.
- H6b: The influence of self-efficacy on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware will be moderated by his or her perception of threat severity.

Threat Susceptibility

Threat susceptibility was also included by Rogers (1975) in his decomposition of the components of a fear appeal as an important element that impacts one's reaction to a fear appeal. Similar to the logic which dictates that the perceived severity of a threat moderates the relationships between an end user's attitude and his or her perceptions of response efficacy and self-efficacy, an end user's perceptions of the probability of encountering the threat also provide such moderation (Rogers, 1975; Witte, 1992). If considered within the context of spyware defense, it is expected that attitudes toward a particular anti-spyware solution based on its ability to effectively and efficiently provide protection will increase in strength as the threat of such an attack becomes more probable. As such, the following hypotheses are offered:

- H7a: The influence of response efficacy on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware will be moderated by his or her perception of threat susceptibility.
- H7b: The influence of self-efficacy on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware will be moderated by his or her perception of threat susceptibility.

Relationships between Source Credibility and Perceptions of Threat and Efficacy

As previously described, the effectiveness of persuasive messages is due in part to the perceived credibility of the source (Bannister, 1986; Suzuki, 1978). The majority of research concerning source credibility employs either the McCroskey and Jenson Source Credibility Scale (McCroskey & Jenson, 1975) or the Leathers Personal Credibility Scale (Leathers, 1992), the latter of which looks at competence, trustworthiness, and dynamism as dimensions of source credibility. Hewgill and Miller's (1965) work probably provides the most insight into the interaction of source credibility and perceived threat resulting from fear appeals. Their investigations of the overall influence of source credibility on perceived threat revealed highly credible sources as more influential in conveying a perception of threat among their audiences than low credible sources (Hewgill & Miller, 1965).

Source Competence

Hewgill and Miller (1965) contend that the credibility of the source of a fear appeal will have an impact on the degree to which the appeal is able to affect change in end user attitudes and behavioral intentions. Mugny et al. (2000) argue that credible sources are more effective than noncredible sources in affecting positive change in

attitudes and behavioral intentions. Competency is an important dimension of source credibility as defined by Leathers (1992). Consider, for example, a fear appeal originating from the office of the Chief Security Officer (CSO) for an organization in which the end user is employed, and another coming from an Intern. It is expected that the CSO will be regarded as highly competent by those end users within his or her organization. This trait should result in a more positive reception of the CSO's message. Alternatively, the Intern's message is more likely to be discarded based on perceptions of his or her lack of competence.

In that appraisals of threat and efficacy are the initial processes that occur in evaluating a fear appeal (Witte, 1992), it is expected that source competence will have a direct influence on an end user's appraisals of threat severity, threat susceptibility and the efficacy of a recommended response. As such, the following hypotheses are offered:

- H8a: The perceived competence of a fear appeal source will have a significant positive effect on an end user's perception of spyware severity.
- H8b: The perceived competence of a fear appeal source will have a significant positive effect on an end user's perception of spyware susceptibility.
- H8c: The perceived competence of a fear appeal source will have a significant positive effect on an end user's appraisal of the efficacy of anti-spyware software.

Source Trustworthiness

A second dimension of source credibility (Leathers, 1992), the trustworthiness of a fear appeal source is also expected to have a significant impact on an end user's perception of threat and response efficacy. Hovland et al. (1953) describe trustworthiness as the degree to which a message recipient believes a communicator's message as being

valid. These authors contend that highly trustworthy sources' arguments are more readily accepted than that of low-trustworthy sources (Hovland & Weiss, 1951). For the purposes of this study, the communicator's message is a fear appeal containing statements of threat severity, susceptibility and anti-spyware efficacy. In terms of resultant perceptions of threat severity and threat susceptibility, as well as perceptions of the efficacy of a recommended response, a trustworthy communicator is expected to provide a more credible message. Based on this expectation, the following hypotheses are offered:

- H9a: The perceived trustworthiness of a fear appeal source will have a significant positive effect on an end user's perception of spyware severity.
- H9b: The perceived trustworthiness of a fear appeal source will have a significant positive effect on an end user's perception of spyware susceptibility.
- H9c: The perceived trustworthiness of a fear appeal source will have a significant positive effect on an end user's appraisal of the efficacy of anti-spyware software.

Source Dynamism

Recall that dynamism refers to the degree to which a source is able to project an image of energy, power, forcefulness or attractiveness (Larson, 1992). It is expected that these qualities enable an advocate for anti-spyware to be more effective in terms of establishing in the minds of others that the potential for spyware is great, and the dangers associated with it are severe. Additionally, it is expected that the dynamism of the source will influence the end user's determination of the capabilities of a recommended action to avert a threat. Based on this expectation, the following hypotheses are offered:

- H10a: The perceived dynamism of a fear appeal source will have a significant positive effect on an end user's perception of spyware severity.

- H10b: The perceived dynamism of a fear appeal source will have a significant positive effect on an end user's perception of spyware susceptibility
- H10c: The perceived dynamism of a fear appeal source will have a significant positive effect on an end user's appraisal of the efficacy of anti-spyware software.

Summary

From the review of the literature, it is evident that the three primary theoretical components of this research (EPPM, UTAUT, and source credibility) are well established in social science research. Based on a synthesis of these research components, a conceptual research model was developed which serves to explain and predict the influence of fear appeals on the compliance of end users with recommendations which articulate specific computer security actions toward the amelioration of threats. From this model, hypotheses were formed that articulate specific contentions of relationships among the latent variables in the model.

CHAPTER III

RESEARCH METHODS

Chapter 3 provides a discussion of the methods employed in this study.

Beginning with a review of the variables of interest in the study's proposed conceptual model, the chapter offers definitions and literary sources for each. Next, this chapter includes descriptions of the study's data collection instrument followed by an overview of the study's two-phase investigation procedure. The preliminary investigative procedure is described; including details of tests of experimental treatment content validity, instrument content validity, and instrument construct validity. A description of a pilot study is also included in this preliminary investigation section. Finally, a discussion of the primary investigation phase of this study is provided, including details of the experimental design, experimental process, and sampling frame.

Variables

The Extended Parallel Process Model (EPPM), the Unified Theory of Acceptance and Use of Technology (UTAUT), and source credibility literature provide the theoretical foundation from which to identify and investigate the latent variables that determine the acceptance and engagement of recommended individual computer security actions. While UTAUT was originally intended to describe a user's acceptance and use of

technology within an organization, this study applies the model within the context of computer security and adapts it through the introduction of EPPM and source credibility.

One dependent variable of interest in this study is behavioral intent. Behavioral intent represents a user's probability of accepting and acting upon a recommended individual computer security action. Based on Fishbein and Ajzen's (1975) Theory of Reasoned Action (TRA), attitude is a determinant of behavioral intent, which is a determinant of behavior. Attitude is itself a dependent variable of interest in this study. Table 3.1 provides definitions for each of these outcome variables. The definitions provided in the table are reflective of the context of this research, and as such are specific to the influence of fear appeals on an individual's actions concerning spyware defense.

Table 3.1 Dependent Variables of Interest

Variable	Definition
attitude	the inclination an end user possesses to react positively or negatively toward a recommended individual computer security action to avert spyware
behavioral intent	the self-reported probability that an end user will adopt a recommended individual computer security action to avert spyware

While an independent variable for the determination of behavioral intent, attitude is also a dependent variable that is explained by constructs as derived from EPPM. Attitude represents a user's cognitive and affective disposition toward a recommended computer security action and is determined by the two dimensions of perceived efficacy,

response efficacy and self-efficacy. The relationships between attitude and the two dimensions of perceived efficacy, the constructs of performance expectancy and social influence are moderated by two dimensions of perceived threat, threat severity and threat susceptibility. Additionally, perceived threat and response efficacy are directly influenced by source credibility; therefore, source credibility is considered an indirect determinant of attitude. Table 3.2 provides definitions for each of the constructs involved in predicting attitude. Similar to the definitions of antecedents of behavioral intent provided in Table 3.1, these definitions are within the context of spyware defense.

Instrument Design

Nine constructs were measured in this study: behavioral intent, attitude, social influence, performance expectancy, perceived efficacy (both response efficacy and self-efficacy), perceived threat (both threat severity and threat susceptibility), and source credibility. The constructs were measured using multi-item scales drawn from validated measures in information systems (IS) acceptance or fear appeal research and are rearticulated to relate specifically to the context of recommended individual computer security action in response to spyware. Additionally, descriptive demographic questions including experience with anti-spyware software, gender, age, education, and department were included in the instrument.

Table 3.2 Determinants of Attitude

Variable	Definition
performance expectancy	the degree to which an end user believes the adoption of anti-spyware actions will enhance his or her performance
social influence	the degree to which the end user perceives his or her friends, relatives, colleagues, and others whose opinions matter, support a recommended individual computer security action to avert spyware
response efficacy	the degree to which an end user believes a recommended response will efficiently and effectively avert spyware
self-efficacy	the degree to which an end user believes he or she is able to perform a recommended action to avert spyware
threat susceptibility	the degree to which an end user believes a spyware threat to be probable
threat severity	the degree to which an end user believes a spyware threat to be severe
source credibility	the degree to which an individual is considered to be competent, trustworthy, and dynamic regarding a specific topic of interest

Witte (1996) contends that in order for the fear appeals to be considered effective, perceptions of threat severity should be described as severe, serious, and significant, while perceptions of threat susceptibility should be described as risky, likely, and possible. A measure of perceived efficacy should address the dimensions of self-efficacy and response efficacy. Perceptions of self-efficacy should be described in terms of the efficiency of adopting a recommended action, while perceptions of response efficacy should be described in terms of the effectiveness of the action. The scale items to

measure threat severity, threat susceptibility, self-efficacy, and response efficacy were developed by Witte (1996) and are utilized frequently in studies related to effective health communications (Witte et al., 1996; Witte & Morrison, 1995). The majority of studies involving these scales consider threat severity and threat susceptibility as two dimensions of perceived threat. Chronbach's alpha for the two dimensions was measured at .90 and .85 respectively (Witte et al., 1996). Also, self-efficacy and response efficacy are described as dimensions of perceived efficacy. Reliability measures for these two dimensions are not reported by Witte et al. (1996).

Table 3.3 provides factor loadings for scale items included in Witte's Risk Behavior Diagnosis scale (Witte et al., 1996). Witte's (1996) study considered items as having loaded significantly on their underlying constructs if their factor loadings exceed .30. While only the item "able." did not load significantly on its intended factor of self-efficacy, Witte (1996) argues that the χ^2 goodness of fit between the four factors, with "able" as an item of self-efficacy, and the observed data were significant so as to justify its position.

Table 3.3 Factor Loadings for Scale Items Used to Measure Threat Severity, Threat Susceptibility, Response Efficacy, and Self-efficacy

Determinant	Severity	Susceptibility	Response Efficacy	Self-Efficacy
threat severity ($\alpha = .90$)				
severe	.90	.26	.31	.47
significant	.79	.26	.22	.37
serious	.90	.23	.17	.50
threat susceptibility ($\alpha = .85$)				
likely	.26	.82	.01	.21
at risk	.20	.90	.10	.29
possible	.27	.81	.01	.29
response efficacy*				
effective	.23	.01	.93	.37
work in preventing	.20	.00	.87	.33
less likely to get	.26	.10	.79	.49
self-efficacy*				
convenient	.37	.23	.16	.57
easy	.20	.16	.02	.55
able	.16	.05	.46	.27

Source: 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*, 317-341.

* individual measures of reliability were not available

Scale items intended to measure the latent variables, social influence, performance expectancy, attitude and behavioral intent were drawn from the work of Venkatesh et al. (2003) in their development of the UTAUT model. Table 3.4 presents factor loadings as determined by Venkatesh et al. (2003) for each of the determinants. Based on tests at three different time periods, Chronbach's alpha measures are also included for each construct, and demonstrate good reliability. Venkatesh et al. (2003)

argued that these items “adequately represented the conceptual underpinnings of the constructs” (p. 457).

Because of the unique context of this study, additional items were included with those used by Venkatesh et al. (2003) in the operationalization of performance expectancy. Within the context of individual computer security actions, performance gains provided by the recommended actions are indirect. For example, security actions such as improved access controls do not directly increase the quantity or quality of the end users’ work. However, these actions can increase the integrity of the output and can reduce the amount of future effort necessary to address confidentiality issues. To ensure that there are at least three items that load together for this construct, it is advisable to include additional items. As such, the next two highest loading items from the UTAUT study were added to the four original items. These items in their original form are included in Table 3.4.

Finally, the semantic differential scale items used to measure source credibility were taken from the Leathers Personal Credibility Scale (Leathers, 1992). Validated in Berlo and Lemert’s (1961) factor analytic research on source credibility, these scales represent the three dimensions of competence, trustworthiness and dynamism. Table 3.5 displays Berlo and Lemert’s factor loadings of these scales. Chronbach’s alpha results of the Leathers Personal Credibility Scale, as reported by Powell and Wanzenried (1995), range from .88 to .94 over 4 different testing periods. These values indicate good reliability.

Table 3.4 Factor Loadings for Scale Items Used to Measure Social Influence, Performance Expectancy, Attitude, and Behavioral Intent

Determinant	Item	Factor Loadings		
		T1	T2	T3
social influence ($\alpha = .88$)*	1) People who influence my behavior think that I should use the system	.82	.85	.90
	2) People who are important to me think that I should use the system	.83	.85	.84
	3) The senior management of this business has been helpful in the use of the system	.84	.80	.90
	4) In general, the organization has supported the use of the system	.80	.82	.84

performance expectancy ($\alpha = .92$)* **	1) I would find the system useful in my job	.88	.88	.90
	2) Using the system enables me to accomplish tasks more quickly	.87	.90	.90
	3) Using the system increases my productivity	.86	.88	.94
	4) If I use the system, I will increase my chances of getting a raise	.86	.87	.90
	5) Using the system would improve my job performance	.84	.80	.81
	6) Using the system would make it easier to do my job	.81	.78	.84

attitude ($\alpha = .84$)*	1) Using the system is a good/bad idea	.80	.83	.85
	2) The system makes work more interesting	.79	.77	.84
	3) Working with the system is fun	.84	.83	.84
	4) I like working with the system	.82	.85	.82

behavioral intent ($\alpha = .92$)*	1) I intend to use the system in the next <n> months	.88	.84	.88
	2) I predict I would use the system in the next <n> months	.82	.86	.88
	3) I plan to use the system in the next <n> months	.84	.88	.87

Source: 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.

* Internal Consistency Reliability at time interval T1

** Internal Consistency Reliability for four item scale

Table 3.5 Factor Loadings for Scale Items Used to Measure Source Competence, Source Trustworthiness, and Source Dynamism

Dimension	Scale	Factor Loading
competence	experienced – inexperienced	.90
	expert – ignorant	.90
	trained – untrained	.90
	competent – incompetent	.88
trustworthiness	just – unjust	.82
	kind – cruel	.78
	admirable – contemptible	.77
	honest – dishonest	.75
dynamism	aggressive – meek	.73
	bold – timid	.72
	energetic – tired	.65
	extroverted – introverted	.64

Source: Hewgill, M. A., & Miller, G. (1965). Source Credibility and Response to Fear-Arousing Communications. *Speech Monographs*, 32(2), 95-101.

A Two-Phase Investigation

This study involved a two-phase investigation in which two separate data samples were collected and analyzed. A preliminary investigation was undertaken for the purposes of validating the research instrument and experimental treatment used in the primary investigation, as well as for conducting a pilot study. Included in these analyses was an exploratory factor analysis (EFA) of the research instrument that involved responses from an independent sample of 200 undergraduates in the College of Business and Industry at Mississippi State University. The primary investigative phase involved tests of the validity of the research design and the conceptual model based on responses from 341 faculty, staff, and students at Mississippi State University. The choice of PCA

as an EFA technique was made in order to be consistent with the recommendations of IS research as put forth by Gefen, Straub, and Boudreau (2000). Structural Equation Modeling (SEM) was also used in the primary phase to conduct a confirmatory factor analysis (CFA) of the instrument and tests of the hypothesized measurement and structural models.

Preliminary Investigation

Prior to the primary data collection efforts, three preliminary tests were conducted to ensure that the instrument, treatment, and experimental procedure were appropriate, accurate, and reliable for the purposes of this research. The preliminary tests included: (a) content validity tests of both the instrument and the experimental treatment; (b) construct validity and reliability tests, including convergent and discriminant validity tests of the scale items used to measure the underlying constructs of the conceptual model; and (c) a pilot study to ascertain the proper working condition of the experimental procedure.

Experimental Treatment Content Validity

A fear appeal must relay to its audience the severity of a threat as well as their susceptibility to the threat. In this case, the threat was invasive software referred to as spyware that has the potential to monitor and capture sensitive information from an unprotected computer system. Along with language or depictions concerning the threat, a fear appeal must include a recommended course of action to avert the threat. For this study the recommended action was to install and run anti-spyware software; that would

detect and remove any instances of spyware found on a system and would provide protection from future spyware intrusions. In conjunction with the recommended action, a fear arousing communication must appeal to its audience's sense of efficacy, both of self and of the response. Therefore, statements to encourage and support the abilities of the respondents as well as the ability of the anti-spyware software were included in the fear appeal.

The experimental manipulation used in this study was accomplished via a typed message in conjunction with a streaming video, both originating from an actor directed to be a University Information Technology Services (ITS) official. Both mediums featured a spyware protection theme and were identical in terms of the specific language of the statement. Each treatment was located on a website maintained within the University's domain as to ensure availability and consistency.

As depicted in Table 3.6, the fear appeal treatment included statements regarding concerns of severity and susceptibility associated with spyware. Spyware refers to computer software that is intended to collect and relay information concerning an end user without the user's awareness or consent. Spyware represents a current and increasingly significant threat to computing environments (Landesman, 2005). The National Cyber-Security Alliance claims that approximately 91% of all home personal computers are infected with some form of spyware (Network Associates, 2004). In fact, spyware has become so pervasive that many states are considering legislation against it (Rapoza, 2005).

Table 3.6 Experimental Treatment Fear Appeal Components

Component	Representative Text
threat severity	potentially harmful to the integrity of the computer's data
threat susceptibility	91% of all home PCs are infected
self-efficacy	the software is easy to install
response efficacy	automatically detect and remove existing installations of spyware

In order to highlight the severity of spyware, statements that describe its potential to capture sensitive information or to cripple the performance of the computer were included in the fear appeal treatment. Furthermore, the personal consequences associated with such an infection were articulated in the message by describing the potential for identity theft or fraud. Concerns of susceptibility to spyware were addressed in the fear appeal treatment by highlighting statistics that underscore the pervasive nature of the threat. Two other components of a fear appeal treatment are self-efficacy and response efficacy. Commentary in support of the ability of the end user to easily install and run anti-spyware software as advocated in the recommended response was included in the message. Statements in support of the effectiveness of the anti-spyware software were also included in the message.

In conjunction with the typed message, a streaming video of an actor advocating the use of anti-spyware software was prepared. The script of the video message was identical to that of the typed message. A tenant of media richness theory (Daft & Lengel,

1986) is that media vary in richness or their ability to convey meaning within a given time period (Dennis & Kinney, 1998). Daft and Lengel (1986) argue that lean media, such as the typed message experimental treatment for this study, should be augmented with a richer form of media such that multiple cues (e.g., voice inflection, facial expression, gestures) are included in the communication. For equivocal tasks, such as attempting to influence end user attitudes and behavioral intentions through the use of a fear appeal, the use of varying modes of communication are highly effective (Daft, Lengel, & Trevino, 1987). To this end, the actor was video recorded reciting a rehearsed, scripted fear appeal which, identical to the typed message, included efficacy and threat components in addition to the recommended response. The streaming video was made available in the three most common formats: Real Player, QuickTime, and Windows Media Player.

In order to establish the validity of the fear appeal treatment, it was subjected to a panel of experts in the field of marketing to gauge its ability to convey certain information considered necessary in a fear appeal. The expert panel consisted of 8 faculty and Ph.D. students in the Department of Marketing, Quantitative Analysis and Business Law at Mississippi State University who have been exposed to fear appeal literature. Upon review, the panel made suggestions for clarity and improvement in conveying threat and efficacy. The final rendition of the fear appeal treatment is included in Appendix C.

Instrument Content Validity

As described by Boudreau, Gefen, and Straub (2001), instrument validation is a necessary, yet all too frequently missing condition for any positivist, quantitative research in which data is gathered and interpreted in search of truth. According to Boudreau et al. (2001), only 26% of articles from the top IS journals sampled in 2001 utilize a form of content validity. Fowler (1984) supports this contention and argues that regardless of the talents or reputation of the researcher, all research instruments should be pretested. As such, preliminary tests of the instrument utilized in this study were conducted to ensure against any potential difficulties that may threaten the research (Alreck & Settle, 1995).

Content validity seeks to establish that the instrument adequately “captures the essence of the construct” (Straub, Boudreau, & Gefen, 2004, p. 12). The goal is to select measures that represent the construct while not including those measures that may cause measurement error. Although content validity is not a perfect science and can be highly subjective, it does provide some assurance that the instrument items used to measure a construct are appropriate for their respective constructs (Straub et al., 2004). Straub (1989, 2004) contends that iterations of the instrument based on feedback from an expert panel are appropriate for establishing content validity.

In conjunction with the previous review of the relevant literature, content validity was established through a panel of 8 experts in the field of quantitative analysis and quantitative research methods. The expert panel consisted of faculty and Ph.D. students from the departments of Management and Information Systems and Marketing, Quantitative Analysis and Business Law at Mississippi State University. These panel

members frequently engage in survey research and have experience assessing content validity. Following a review of the instrument, the panel made several suggestions to improve the instrument in terms of the order and language of the items and verbage of the instructions. The instrument was iterated accordingly. Its final version is presented in Appendix B.

Construct Validity and Reliability

In order to ensure that the instrument items were a reasonable operationalization of their respective constructs, construct validity tests were conducted. An independent sample of 200 undergraduate students from the College of Business and Industry at Mississippi State University was administered the questionnaire (without source credibility scales). The responses were analyzed using an exploratory factor analysis (EFA) technique, PCA. Component loadings were examined to ensure that items loaded cleanly on those constructs to which they were intended to load and did not cross-load on constructs to which they should not have loaded (Straub et al., 2004). Generally, convergent validity is demonstrated if the item loadings are in excess of .70 on their respective factors, and discriminant validity is demonstrated if the factor loadings are less than .40 on unintended factors (Gefen, Straub, & Boudreau, 2000). Results of the EFA are presented in Chapter 4.

It is important to note that the use of factor analysis to perform tests of convergent and discriminant validity is a limitation. Although the majority of research in the field of IS utilizes factor analysis as a method for construct validity testing, true validity tests are

theory driven. Factor loadings for an item only provide a correlation of that item with other items, with no ability to define a construct.

Pilot Study

As a final element of the preliminary investigation, a pilot study involving a randomly selected group of 12 faculty, staff, and students from Mississippi State University was conducted. The purpose of the pilot study was to ensure that the procedures and technologies employed in the data collection process were properly established. The participants of the pilot study stepped through the entire data collection process in an effort to identify and report flaws or inconsistencies in the process. One example of a reported flaw was concerning the clarity of the instructions for answering the first three items of the survey. These items were intended to filter out those subjects that did not engage in the protection of a computer system, thereby rendering themselves immune to communicated warning of impending danger. It was unclear whether the potential respondent should consider his or her responsibility to a personal computer or to a primary work-related computer. This and other problems identified by the panel were corrected accordingly.

Primary Investigation

Following the preliminary investigation involving tests of the research instrument, experimental treatment, and research process, the primary phase of the investigation based on a Solomon four-group design was invoked. The data collected in this sample were used to empirically test the proposed conceptual model as illustrated in Figure 2.5.

The Structural Equation Modeling (SEM) approach to data analysis was used in this phase of the study, as it has been described as particularly appropriate for testing theoretically justified models because it provides for simultaneous evaluation of measurement quality as well as the causal relationships between constructs (Bentler & Bonnett, 1980; Bhattacharjee, 2001). Therefore, SEM techniques provide for more rigorous and flexible testing of complex predictive models than comparable multiple regression techniques (Kelloway, 1998). Table 3.7 depicts the hypotheses tested in the present research and their respective statistical measures that, if true, signify support. At a .05 level of significance, the relationship between an exogenous variable (independent variable) and an endogenous variable (dependent variable) is considered significant if the t-value for γ is greater than or equal to 1.96. For endogenous variable to endogenous variable relationships, significance is found if the t-value for the β parameter is greater than or equal to 1.96 at the .05 level of significance.

Table 3.7 Hypotheses and Model Estimation Components

Hypotheses	Structural Relationship	Parameter to be Estimated
H1	attitude has a <i>positive</i> influence on behavioral intent	β_1
H2	social influence has a <i>positive</i> influence on attitude	γ_1
H3	performance expectancy has a <i>positive</i> influence on attitude	γ_2
H4	response efficacy has a <i>positive</i> influence on attitude	β_2

Table 3.7 (continued) Hypotheses and Model Estimation Components

Hypotheses	Structural Relationship	Parameter to be Estimated
H5	self-efficacy has a <i>positive</i> influence on attitude	γ_3
H6a	a higher threat severity makes response efficacy have a stronger positive influence on attitude	γ_{4H}
	a lower threat severity makes response efficacy have a weaker positive	γ_{4L}
H6b	a higher threat severity makes self-efficacy have a stronger positive influence on attitude	γ_{5H}
	a lower threat severity makes self-efficacy have a weaker positive influence on attitude	γ_{5L}
H7a	a higher threat susceptibility makes response efficacy have a stronger positive influence on attitude	γ_{6H}
	a lower threat susceptibility makes response efficacy have a weaker positive influence on attitude	γ_{6L}
H7b	a higher threat susceptibility makes self-efficacy have a stronger positive influence on attitude	γ_{7H}
	a lower threat susceptibility makes self-efficacy have a weaker positive influence on attitude	γ_{7L}
H8a	source competence has a <i>positive</i> influence on threat severity	γ_8
H8b	source competence has a <i>positive</i> influence on threat susceptibility	γ_9
H8c	source competence has a <i>positive</i> influence on response efficacy	γ_{10}

Table 3.7 (continued) Hypotheses and Model Estimation Components

Hypotheses	Structural Relationship	Parameter to be Estimated
H9a	source trustworthiness has a <i>positive</i> influence on threat severity	γ_{11}
H9b	source trustworthiness has a <i>positive</i> influence on threat susceptibility	γ_{12}
H9c	source trustworthiness has a <i>positive</i> influence on response efficacy	γ_{13}
H10a	source dynamism has a <i>positive</i> influence on threat severity	γ_{14}
H10b	source dynamism has a <i>positive</i> influence on threat susceptibility	γ_{15}
H10c	source dynamism has a <i>positive</i> influence on response efficacy	γ_{16}

Experimental Design

As described by Leventhal (1970), the typical experimental design for studies concerning the impact of fear appeals on attitude and/or behavioral intent is the classical design whereby participants are exposed to some form of communication and questioned as to the impact of the stimulus prior to and after the treatment. For example, in Roskos-Ewoldsen, Yu, and Rhodes' (2004) experiment to determine the influence of fear-inducing persuasive messages on attitudes and behaviors regarding breast cancer prevention techniques, the researchers subjected female research participants to printed messages regarding the threat of breast cancer and the efficacy of self-examination. Prior

to and after the exposure to the fear appeal, the participants were tested to gauge attitude and behavioral intent.

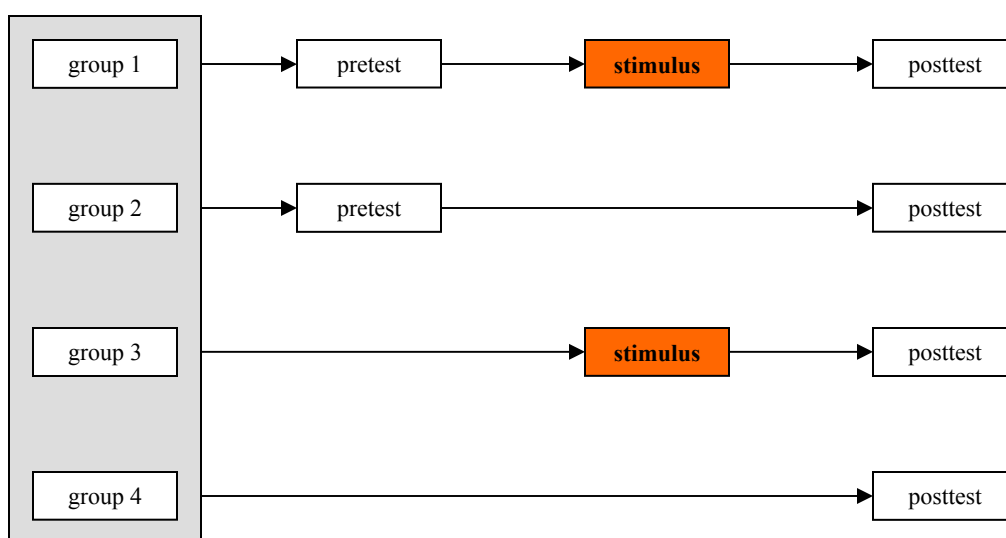
Through the use of a control group, the classical design provides adequate assurance that any change in behavioral intent or attitude is the result of the treatment as opposed to sources of internal validity such as history, maturation effect, or testing (Babbie, 2004; Campbell & Stanley, 1963; Cook & Campbell, 1979). However, sources of external validity such as interaction between the testing conditions and the treatment remain a problem for the classical experiment design (Babbie, 2004).

History can affect the results of the experiment by altering perceptions regarding the treatment based on events that occur during the timeframe of the experiment. Also a product of longevity, maturation can influence the results of an experiment. As people gain experience, mature, and learn, their perceptions regarding a specific stimulus may change as well. Another source of contamination of experimental results is found in the process of testing and retesting of participants' attitudes or behaviors. The time period between the pretest and posttest could allow for the participants to form expectations based on what they perceive to be the measurement of interest. Additionally, the circumstances in which an experimental treatment is conducted may have an effect on the results of the experiment. Within the classical experimental design, it is difficult to determine if the treatment would have generated the same response if applied under difference conditions or circumstances.

As a means for controlling for these validity issues, this study employed a quasi-experimental Solomon four-group design (Campbell & Stanley, 1963) to determine the

effect of fear appeals on the compliance of end users with recommendations which advocate the use of anti-spyware software toward the amelioration of spyware. This design required four groups of subjects to be randomly assigned from the general pool of participants. As depicted in Figure 3.1, the design was intended to control for any interaction that may occur between the testing and the experimental stimulus, in this case a fear appeal (Babbie, 2004). For example, it was expected that a fear appeal would influence the attitudes and intentions concerning recommended individual security actions for those groups to which it is applied. However, only through the posttest measures of control groups was it possible to be assured that the fear appeal treatment, rather than the conditions associated with the fear appeal treatment, was responsible for the modified attitudes and intentions.

The Solomon four-group design allows the researcher to control for problems of internal validity and external validity. By controlling for internal validity, the researcher is assured of equivalence between groups and holds a high degree of confidence that the posttest observed measures are in fact caused by the treatment as opposed to issues of history, maturation effect, or testing. Problems relating to history, maturation, and testing are addressed by the use of a control group that is not exposed to the treatment. As long as participants are randomly assigned to groups 1 and 2, any impact of history, maturation, or testing is felt by both groups. Comparisons of differentials between groups 1 and 2 and groups 3 and 4 convey any interaction between the testing and stimulus (Babbie, 2004).



Source: Adapted from Babbie, E. (2004). *The Practice of Social Research* (10 ed). Belmont, CA: Wadsworth/Thomson Learning.

Figure 3.1

Solomon Four-Group Design

Experimental Procedure

Based on the requirements as dictated by the Solomon four-group design as well as the requirements of SEM, the primary data collection effort involved the collection of data from 341 respondents from a random sample of approximately 780 University faculty, staff, and students. The subjects were contacted via email asking if they would be willing to voluntarily participate in a research project. The email contained a link to a website that served as the medium for conducting the experiment. If a participant followed the link, the first screen he or she encountered on the website was an electronic consent form. If the participant elected to participate in the experiment by selecting the appropriate link on the consent form, the next screen the participant encountered was

dependent upon the experimental group to which he or she was randomly assigned. For reasons relating to experimental design and data analysis, the participants were randomly assigned to four groups such that group 1 had, at a minimum, an n of 200, and groups 2 through 4 each had at least an n of 30. These group sizes would allow for tests of internal and external validity (based on the Solomon four-group design) to be conducted using a minimum of 30 responses from each group, and allow for SEM tests of the conceptual model to be conducted based on a sample size of no less than 200 responses in group 1.

In addition to the collection of demographic information concerning experience, gender, age, education, and department, the experimental procedure involved a preliminary assessment of self-reported perceptions of response efficacy, self-efficacy, threat severity, threat susceptibility, social influence, attitude, and behavioral intent toward a recommendation to address a specific form of computer threat, spyware. This pretest was conducted using two of the randomly assigned groups of participants, group 1 and group 2. Only if the participant was randomly assigned to either one of these groups would he or she have viewed a pretest instrument designed to measure those latent variables as previously described.

Next, an experimental treatment, in the form of a fear appeal originating from a highly experienced, University technology expert, was applied to group 1 as well as group 3. This fear appeal consisted of a typed statement and a streaming video. Only if the participant was randomly assigned to group 1 or group 3 would he or she have viewed the experimental treatment. Following the review of both forms of the treatment, the group 1 and group 3 participants were asked to verify that they had in fact viewed the

typed document as well as the streaming video. Those respondents that were unable to view the video were dismissed from the study.

Finally, a posttest measure of the same latent variables involved in the pretest assessment was taken of all groups, including a fourth group (group 4) that had not been subjected to either the pretest or the treatment. The posttest assessment for groups 1 and 4 included a section regarding source credibility (section 3 of the instrument).

As described in the following chapter, the results of the experiment were analyzed using between subjects analysis of variance to determine if the differences in latent variable measurements from the initial assessment to the final assessment were in fact due to the treatment. The dependent variable for the analysis was attitude. For groups 2, 3, and 4, the sample space was only 30; however, for group 1, a random sample of 30 from the 200 was taken. Following the ANOVA, the remaining sample of group 1 participants were added to the initial 30 to form of total sample space of 215 subjects for the SEM testing.

Sampling Frame

The primary investigation phase of this study involved the collection of responses from faculty, staff, and students at Mississippi State University. This particular sampling frame was chosen due to its quality representation of knowledge workers found in corporate environments or other domains in which higher education is preferable among employees. The participants were technology users involved in coping with threats to the security of their personal digital assets. Furthermore, these subjects varied in terms of efficacy, age, and anti-spyware experience levels. Considering that this study involved

perceptions of various constructs formed from cognitions and emotions concerning a communicated message and that the threat and recommended response mirror actual events, findings based on this sample should be generalizable to the greater population of technology users.

Initially defined by Druker (1959), knowledge workers are those that engage in activities toward the development or use of knowledge, typically through the application of information technology. Based on this definition and supported in the works of Deem (2004) and Trow (1993), university faculty, staff, and students are considered knowledge workers. However, for the purposes of this study, a particular type of knowledge worker was necessary, the end user of technology or those that were positioned as consumers of technical resources as opposed to those that developed or created the technology. The technologies of interest were computer systems and computer security technologies in support of spyware detection, protection, and remediation.

The general computing environment provided for the employees and students at Mississippi State University encourages the operator of individual assigned personal computers to install and maintain software for the express purpose of preventing, detecting and removing malicious software. Exceptions to this practice are found in computer laboratory environments. It is a goal of the University to provide the facilities and infrastructure from which its employees and students can successfully meet their respective computing requirements. It was therefore expected that faculty, staff and students have access to at least one system, whether personally owned or university provided, within which they store and manipulate data they consider to be critical to their

success as employees or students. Additionally, for the purposes of this study it was necessary for the participants to regard themselves as having some degree of responsibility for the security of their computing facilities; otherwise, they would not regard any threat as relevant.

To be sure that a prospective research participant met the two requirements of (a) access to at least one computer system within which he or she maintains important data; and (b) at least partial responsibility for security of the system, three questions were posed prior to primary data collection that addressed these requirements. These questions were included in the research instrument as provided in Appendix B.

Summary

This chapter described the two-phase investigation used in this study. The first phase was a preliminary investigation in which tests of instrument and experimental treatment content validity and instrument construct validity were performed. Also included in the preliminary investigation was a pilot study. The second phase of the study was the primary investigation. This chapter outlined the experimental design and process of this phase and concluded with a description of the characteristics of the data sample. The next chapter presents the results of the EFA conducted as part of the preliminary investigation and of the analysis of data collected as part of the primary phase of investigation. Tests of internal and external validity as dictated by a Solomon four-group design, and tests of the measurement and structural models performed using SEM are included in the analysis.

CHAPTER IV

DATA ANALYSIS AND RESULTS

This chapter is devoted to the reporting of results of tests involved in this study's preliminary and primary phases of investigation. First, results are presented from the exploratory factor analysis (EFA) conducted as part of the preliminary investigation. Next, results from the primary investigation are presented, including tests of internal and external validity based on the Solomon four-group design. Next, a two-stage approach (Anderson & Gerbing, 1988) for testing this study's conceptual model is described. The first stage involved an analysis of the measures from the model in which validity and reliability tests were performed. The second stage involved the test of the structural model. The results of this analysis are described and interpreted in terms of tests of the hypotheses.

Preliminary Investigation Results

As described in Chapter 3, the preliminary investigation of this study involved content validity tests of both the experimental treatment and the instrument. As part of the preliminary investigation, an exploratory factor analysis (EFA) was also conducted to ensure the validity and reliability of the constructs and their respective items included in the instrument. The EFA was conducted using data obtained from an independent sample

of 200 undergraduate students from the College of Business and Industry at Mississippi State University.

Exploratory Factor Analysis

Principle Component Analysis (PCA) revealed findings consistent with the theory that supported the instrument development. As depicted in Table 4.1, component loadings provide evidence of convergent and discriminant validity. Following a Varimax rotation, initial PCA analysis revealed cross-loadings from items PERF1, PERF4, PERF5, PERF6, SIN1, SIN2 and ATTI1. This could be an indication of the general nature of the language of these items, thereby allowing them to be applicable to other construct measurements. For instance, it could be argued that the term “useful” in PERF1 is also applicable for items intended to gauge response efficacy. Following the removal of these variables from analysis, the results were much improved. While item ATTI2 did not load above .70 on its respective component (attitude), its relatively low loadings on the other components suggested that it could remain in the instrument and pose no threat to discriminant validity.

Reliability measures were also acceptable for all constructs. Nunnally (1978) contends that an acceptable level of reliability for applied research is represented by Chronbach’s α in excess of .80. There is no consensus among scholars, however, as to this threshold. According to Shaw and Wright (1967), acceptable levels of reliability are indicated by Chronbach’s α values in excess of .75. Shown in Table 4.1, the standard coefficient of internal consistency, Chronbach’s α , for constructs ranged from $\alpha = .961$

for Behavioral Intent to $\alpha = .787$ for Performance Expectancy. Reliability measures for Performance Expectancy and Attitude further supported the removal of items from analysis in that Chronbach's α for Performance Expectancy was $\alpha = .781$ prior to removal of items PERF1, PERF4, PERF5, and PERF6, and $\alpha = .787$ after removal. Chronbach's α for Social Influence was $\alpha = .800$ before removal of items SINF1 and SINF2, and $\alpha = .856$ after removal. Chronbach's α for Attitude was $\alpha = .781$ prior to removal of item ATTI, and $\alpha = .888$ after removal. The improvements in reliabilities, in addition to the improved component loadings, suggest the removal of these items from analysis was appropriate.

Table 4.1 Verimax Rotated Component Matrix

	Attitude ($\alpha = .888$)	Intent ($\alpha = .961$)	Social Influence ($\alpha = .856$)	Performance Expectancy ($\alpha = .787$)	Self Efficacy ($\alpha = .904$)	Efficacy Response ($\alpha = .882$)	Threat Severity ($\alpha = .852$)	Susceptibility Threat ($\alpha = .844$)
TSEV1	-.012	-.061	-.017	.081	-.054	-.061	-.896	-.011
TSEV2	.015	.032	.069	-.014	-.061	.084	.909	.058
TSEV3	-.042	.200	.123	.007	.022	.066	.778	.134
TSUS1	-.031	.072	-.073	-.034	-.082	-.001	.263	.833
TSUS2	.012	.086	-.072	.092	.101	-.098	.042	.905
TSUS3	-.050	.132	.034	-.083	.021	.087	-.085	.845
SEFF1	-.007	.158	.059	.042	.904	.138	-.078	.050
SEFF2	.152	.135	.123	.054	.858	.086	.018	-.007
SEFF3	.144	.285	.009	.043	.813	.223	-.065	.004
RESP1	.006	.133	.105	.085	.130	.897	.105	.020
RESP2	.000	.110	.186	.183	.210	.808	.014	-.049
RESP3	.088	.180	.102	.083	.090	.850	.134	.020
PERF2	.134	.055	.022	.785	.208	.274	.155	-.081
PERF3	.073	.071	.099	.848	.174	.174	.059	-.012
SINF3	.123	-.002	.826	.060	.116	.073	.088	-.137
SINF4	.094	.185	.757	-.004	.159	.164	.103	-.077
BINT1	.030	.869	.218	.104	.241	.129	.040	.114
BINT2	.015	.921	.140	.055	.160	.168	.086	.117
BINT3	-.004	.906	.137	.069	.203	.161	.066	.119
ATTI2	.575	.103	.369	.338	-.120	-.083	.003	.023
ATTI3	.920	-.051	.091	.084	.057	.012	.015	-.045
ATTI4	.886	.029	.077	.139	.162	.075	-.031	.013
ATTI5	.923	.025	.104	.133	.117	.063	-.025	-.055

Primary Investigation Results

Beginning with a description of the characteristics of the sample, the results of analysis involved in the primary investigation phase of this study are presented. As part of this report, results of tests for internal and external validity of the experimental study are provided. Finally, results from a two-stage process for testing the conceptual model are presented.

Characteristics of the Sample

A sample was drawn from the university during the fall of 2005. Approximately 780 faculty, staff, and students from numerous units within the University were contacted for voluntary participation from which 341 responses were obtained, resulting in a 39% response rate. Responses were obtained from faculty, staff, and students from the College of Business and Industry, Human Resources, Continuing Education, the College of Veterinary Medicine, Department of Sociology, Anthropology and Social Work, Physical Plant, and Information Technology Services (ITS). After removing incomplete or careless responses, the total number of useable responses was 305.

As illustrated in Table 4.2, 61.6% of the respondents were male (38.4% female) with the majority (63.6%) associated with the College of Business and Industry. Approximately six percent (5.9%) of the respondents were from the College of Veterinary Medicine, while 4.3% were from ITS and 25.2% from other undisclosed locations. A large majority (83%) of the respondents was between the ages of 18 and 29. The other age groups were represented as follows: (a) 30 to 39 (8.5%); (b) 40 to 49 (4.3%); and (c) 50 to 59 (4.3%). The majority of respondents reported some college

education (75.4%) without completion of degree requirements. Approximately thirteen percent (13.8%) of the respondents held bachelor's degrees, while only 4.6% hold master's degrees.

Table 4.2 Respondent Demographic Information

Demographic	Count	Percentage
Gender	305	100%
male	188	61.6%
female	117	38.4%
Experience	305	100%
<6 months	96	31.5%
6-12 months	40	13.1%
>1 year to 2 years	55	18.0%
>2 years to 3 years	36	11.8%
> 3 years	78	25.6%
Age	305	100%
18 to 29	253	83.0%
30 to 39	26	08.5%
40 to 49	13	04.3%
50 to 59	13	04.3%
60 and over	0	00.0%
Education	305	100%
high school	11	03.6%
some college	230	75.4%
bachelor's degree	42	13.8%
master's degree	14	04.6%
doctorate	7	02.3%
other	1	00.3%
Affiliation	305	100%
COBI	194	63.6%
CVM	18	05.9%
ITS	13	04.3%
CE	3	01.0%
other	77	25.2%

Tests of Internal and External Validity

As depicted in Table 4.3, the results of a between subjects ANOVA involving group 1 (pretest-treatment-posttest) and group 2 (pretest-posttest) suggest the differential in attitude (group 1 mean = 2.80; group 2 mean = 3.28) was in fact caused by the application of the fear appeal treatment. The significance of .029 implies that the difference in self-reported attitude between group 1 and group 3 was caused by the presence of the fear appeal treatment. A similar test involving group 3 (treatment-posttest) and group 4 (posttest) responses also indicates that the difference in attitude between group 3 (mean = 2.82) and group 4 (mean = 3.20) respondents was caused by the presence of a treatment (see Table 4.4).

Table 4.3 Between Subjects ANOVA for Groups One and Two

	Sum of Squares	df	Mean Square	F	Sig.
Between Subjects	3.384	1	3.384	5.037	.029
Within Subjects	38.969	58	0.672		
Total	42.353	59			

Table 4.4 Between Subjects ANOVA for Groups Three and Four

	Sum of Squares	df	Mean Square	F	Sig.
Between Subjects	2.166	1	2.166	5.093	.028
Within Subjects	24.668	58	0.425		
Total	26.834	59			

To verify that the changes in attitude were not the result of testing conditions (use of a pretest), ANOVA tests were conducted with the same dependent variable attitude, but with the independent categorical variable pretest (1=yes, 0=no). These tests were conducted using a random sample of 30 responses from group 1 (pretest-treatment-posttest) and 30 responses from group 3 (treatment-posttest). The results (see Table 4.5) confirm that the group responses did not differ as a result of the pretest condition. A similar test was performed involving 30 responses from group 2 (pretest-posttest) and group 4 (posttest). The results of this test, shown in Table 4.6, also confirmed that the pretest did not significantly impact the changes in attitude.

Table 4.5 Between Subjects ANOVA for Groups One and Three

	Sum of Squares	df	Mean Square	F	Sig.
Between Subjects	1.838	1	1.838	2.945	.091
Within Subjects	36.188	58	0.624		
Total	38.025	59			

Table 4.6 Between Subjects ANOVA for Groups Two and Four

	Sum of Squares	df	Mean Square	F	Sig.
Between Subjects	0.523	1	0.523	1.181	.282
Within Subjects	25.667	58	0.443		
Total	26.189	59			

Based on these findings, it is clear that at least one outcome variable, attitude, was significantly altered due to the presence of a fear-inducing arguments. Additionally, the application of a pretest did not significantly alter the posttest responses.

The Measurement Model

The data were subjected to confirmatory factor analysis (CFA). According to Kelloway (1996), the use of SEM to conduct confirmatory factor analysis is one of its most common uses. This research followed a two-step analytical process (Anderson &

Gerbing, 1988) in which an analysis of the validity and reliability of measures was performed prior to the analysis of the structural model. The SEM software package, LISREL 8, was used in measurement and structural model testing.

This study involved the measurement of 11 latent constructs via 43 observable indicator variables. Each construct was gauged via multiple indicators. The measurement model specifies the relationships between these indicators and the latent constructs through the loadings of the indicators and their error terms (Kelloway, 1996). Two equations are involved in this analysis, one of which involves endogenous constructs, the other exogenous constructs. The equations are:

$$X = \Lambda_X \xi + \delta \quad (4-1)$$

$$Y = \Lambda_Y \eta + \varepsilon \quad (4-2)$$

where X is an exogenous indicator and Y is an endogenous indicator. The Greek letter, ξ , represents an exogenous construct, while η represents an endogenous construct. Also, Λ_X represents the matrix loadings for the exogenous indicators and Λ_Y represents the matrix loadings for the endogenous indicators. Considering that for the measurement model, endogenous and exogenous variables are not differentiated and all of the indicators are treated as exogenous variables, $X = \Lambda_X \xi + \delta$ is the only equation evaluated (Kelloway, 1996). SEM attempts to solve this equation based on the hypothesized measurement model's parameters and, in doing so, to produce a model-specified variance-covariance matrix, Σ , that most closely replicates the variance-covariance matrix derived from the actual data. This is commonly referred to as measurement model fit to the data.

As a means of describing how well the measurement model fits the data, LISREL provides several indices, such as chi-square χ^2 , root mean square error of approximation (RMSEA) and the goodness-of-fit index (GFI). A heuristic (Chin & Todd, 1995) for model fits is that the fit indices, GFI, AGFI, NFI, NNFI, and CFI should be greater than 0.90, RMSEA should be less than 0.50, and chi-square should be insignificant. Measurement models that meet these criteria are regarded as having “good” overall fit with the data (Chin & Todd, 1995).

Specification and Respecification of the Measurement Model

Table 4.7 shows the specification and respecification process for the conceptual model. In step 1, all 11 reflective scales in the structural model were defined in a measurement model. This is the model after EFA results from the preliminary phase of investigation dictated the removal of items PERF1, PERF4, PERF5, PERF6, SINFI, SINFI2 and ATTI1.

RMSEA was .057 in step 1 and suggested further purification of indicators. In this step, COMP1 shared large residuals with other indicators and was deleted for step 2. With COMP1 deleted in step 2, RMSEA was .053. DYNAM2 shared large residuals with other indicators and was removed in step 3 resulting in an RMSEA of .049. The loadings for DYNAM1 (0.69) were below the suggested level of 0.70 (Fornell & Larcker, 1981) for the expected construct. This indicator was deleted in step 4, and RMSEA remained .049. This value in addition to the other fit indicators, NFI = .85, NNFI = .92, GFI = .80, and CFI = .93, suggests the revised measurement model demonstrated an adequate fit to the data.

Table 4.7 Measurement Model Specification Process

Step	Changes	χ^2	d.f.	RMSEA	NFI	NNFI	GFI	CFI
1	None	1018.49	574	0.057	0.85	0.92	0.80	0.93
2	Deleted COMP1	914.97	539	0.053	0.86	0.93	0.82	0.94
3	Deleted DYNM2	824.74	505	0.049	0.87	0.93	0.83	0.94
4	Deleted DYNM1	720.86	440	0.049	0.88	0.94	0.84	0.95

Scale Assessment and Validation

From the final measurement model described above, convergent validity, discriminant validity, and reliability of all scales were analyzed. Convergent and discriminant validity tests were performed and analyzed according to the recommendations of Fornell and Larcker (1981). According to Fornell and Larcker, convergent validity can be established via CFA by inspecting the λ loadings for items on their constructs, and the average variance extracted (AVE) for the constructs. Lambda (λ) values in excess of .70 and average variance extractions above .50 provide evidence of convergent validity. As depicted in Table 4.8, all item loadings in the CFA model were significant and exceeded .70. As shown in Table 4.9, AVE ranged from 0.69 to 0.81. Hence, the convergent validity of the scales was reasonable. Composite reliabilities of the research constructs also exceeded the .70 threshold, ranging from 0.87 to 0.96.

A comparison of two measurement models, one which limits construct correlations to 1 and another which permits estimation, provides for a detailed analysis of discriminant validity between constructs (Anderson & Gerbing, 1988; Gefen et al., 2000; Segars, 1997). A significant difference between the χ^2 distributions would provide evidence of discriminant validity between the pair of constructs. Gefen et al. (2000) support this analytic technique and its continued emergence in IS research.

As Table 4.9 indicates, there were no intercorrelations above .70 between constructs; therefore, the three highest correlations were tested. It is assumed that if the constructs with the highest correlations can discriminate against each other then those with lower correlations will also discriminate. Table 4.10 shows the results of testing the construct pairs, TRST and COMP, DYNM and COMP, and DYNM and TRST. As the results suggest, all tested pairs of constructs had χ^2 differences above 3.841, thereby providing evidence of discriminant validity at a 95% level of confidence.

Table 4.8 Confirmatory Factor Analysis

Item	Mean	Std Dev	Std Loading	Error Loading
TSEV1	3.82	1.04	0.88	0.23
TSEV2	3.93	0.95	0.96	0.09
TSEV3	4.04	0.87	0.80	0.36
TSUS1	3.70	1.03	0.85	0.28
TSUS2	3.55	1.03	0.87	0.24
TSUS3	3.82	0.89	0.76	0.42
SEFF1	3.75	0.86	0.87	0.25
SEFF2	3.70	0.85	0.91	0.16
SEFF3	3.78	0.84	0.85	0.28
RESP1	4.17	0.82	0.79	0.38
RESP2	3.99	0.87	0.91	0.17
RESP3	4.07	0.73	0.80	0.36
PERF2	3.44	0.92	0.85	0.27
PERF3	3.40	0.92	0.88	0.23
SINF3	3.52	1.02	0.78	0.40
SINF4	3.81	0.93	0.97	0.06
BINT1	4.04	0.85	0.91	0.18
BINT2	4.07	0.85	0.94	0.11
BINT3	4.10	0.77	0.85	0.27
ATTI2	3.08	0.95	0.81	0.35
ATTI3	2.97	0.98	0.92	0.15
ATTI4	3.10	1.04	0.89	0.21
ATTI5	3.03	1.05	0.92	0.15
COMP2	2.69	1.05	0.78	0.39
COMP3	2.42	1.11	0.97	0.05
COMP4	2.44	1.14	0.91	0.17
TRST1	2.94	1.07	0.88	0.31
TRST2	2.95	1.02	0.80	0.36
TRST3	3.17	1.01	0.84	0.29
TRST4	2.80	1.05	0.85	0.28
TRST5	2.88	1.12	0.82	0.33
DYNM3	3.25	1.20	0.92	0.15
DYNM4	3.33	1.33	0.88	0.23

Table 4.9 Reliability, AVE and Inter-Construct Correlations

CONST(#)	RELI	AVE	TSEV	TSUS	SEFF	RESP	PERF	SINF	BINT	ATTI	COMP	TRST	DYNM
TSEV(3)	0.94	0.77	1										
TSUS(3)	0.87	0.69	0.40	1									
SEFF(3)	0.94	0.77	0.15	0.18	1								
RESP(3)	0.88	0.70	0.35	0.11	0.32	1							
PERF(2)	0.92	0.75	0.25	0.30	0.47	0.46	1						
SINF(2)	0.94	0.77	0.32	0.21	0.30	0.38	0.36	1					
BINT(3)	0.96	0.81	0.17	0.15	0.36	0.40	0.24	0.41	1				
ATTI(4)	0.94	0.78	0.15	0.12	0.33	0.12	0.43	0.13	0.04	1			
COMP(3)	0.95	0.80	-0.19	-0.18	-0.20	-0.12	-0.19	-0.17	-0.19	-0.13	1		
TRST(5)	0.88	0.68	-0.11	-0.19	-0.16	-0.10	-0.17	-0.25	-0.13	-0.00	0.61	1	
DYNM(2)	0.96	0.81	-0.29	-0.18	-0.21	-0.16	-0.42	-0.31	-0.13	-0.27	0.52	0.49	1

Table 4.10 Measurement Model Respecification Process

Construct	Freed Model		Constrained Model		Difference	
	d.f.	χ^2	d.f.	χ^2	d.f.	χ^2
TRST and COMP	19	34.81	20	368.84	1	334.03 > 3.841
DYNM and COMP	13	57.66	14	392.50	1	334.84 > 3.841
DYNM and TRST	26	69.52	27	589.18	1	519.66 > 3.841

The Structural Model

The next step involved analysis of the structural model illustrated in Figure 2.5 utilizing the measures resulting from the measurement model analysis. The path coefficient analysis results for the model are shown in Table 4.11 and illustrated in model form in Figure 4.1. Browne and Cudeck (1993) as well as MacCallum et al. (1996) contend that a structural model has adequate fit with the data if the RMSEA is less than 0.08. Based on this contention, the structural model fit adequately with the data with an RMSEA equal to 0.068. Other fit indicator values include $\chi^2 = 592.96$ (d.f. = 300), NFI = 0.87, NNFI = 0.91, GFI = 0.83, and CFI = 0.92.

Tests of the Hypotheses

Table 4.11 shows the results of the structural model analysis in terms of paths. The path from response efficacy to attitude (t-value = 3.10), the path from attitude to behavioral intent (t-value = 3.13), and the path from self-efficacy to attitude (t-value = 4.85) were significant at a .05 level of significance or better, thereby supporting their associated hypotheses. Conversely, the paths from performance expectancy to attitude (t-

value = 1.09), social influence to attitude (t-value = -0.95), source competence to response efficacy (t-value = -1.18), source trustworthiness to response efficacy (t-value = -0.04), and source dynamism to response efficacy (t-value = -1.71) were nonsignificant, thereby not supporting their associated hypotheses.

A test of a structural model containing source competence, source trustworthiness, and source dynamism as modifiers of threat severity and threat susceptibility produced an RMSEA of 0.52 indicating an adequate fit to the data. Other goodness of fit indicator values were $\chi^2 = 149.03$ (d.f. = 94), NFI = 0.94, NNFI = 0.96, GFI = 0.92, and CFI = 0.97. In terms of path analysis, the results indicated no paths were found to be significant.

Table 4.11 Standardized Path Estimates for Proposed Structural Model

Path	Estimate	t-value	p-value
response efficacy → attitude	0.20	3.10	< 0.01
attitude → behavioral intent	0.11	3.13	< 0.01
source competence → response efficacy	-0.13	-1.18	n.s.
source trustworthiness → response efficacy	-0.01	-0.04	n.s.
source dynamism → response efficacy	-0.15	-1.71	n.s.
source competence → threat severity	-0.11	-0.98	n.s.
source trustworthiness → threat severity	0.09	0.88	n.s.
source dynamism → threat severity	-0.28	-3.09	n.s.
source competence → threat susceptibility	-0.08	-0.76	n.s.
source trustworthiness → threat susceptibility	-0.10	-0.95	n.s.
source dynamism → threat susceptibility	-0.09	-0.98	n.s.
self-efficacy → attitude	0.31	4.85	< 0.01
social influence → attitude	-0.31	-0.95	n.s.
performance expectancy → attitude	0.39	1.09	n.s.

$\chi^2 = 592.96$ (d.f. = 300)
 RMSEA = 0.068, NFI = 0.87, NNFI = 0.91, GFI = 0.83, and CFI = 0.92

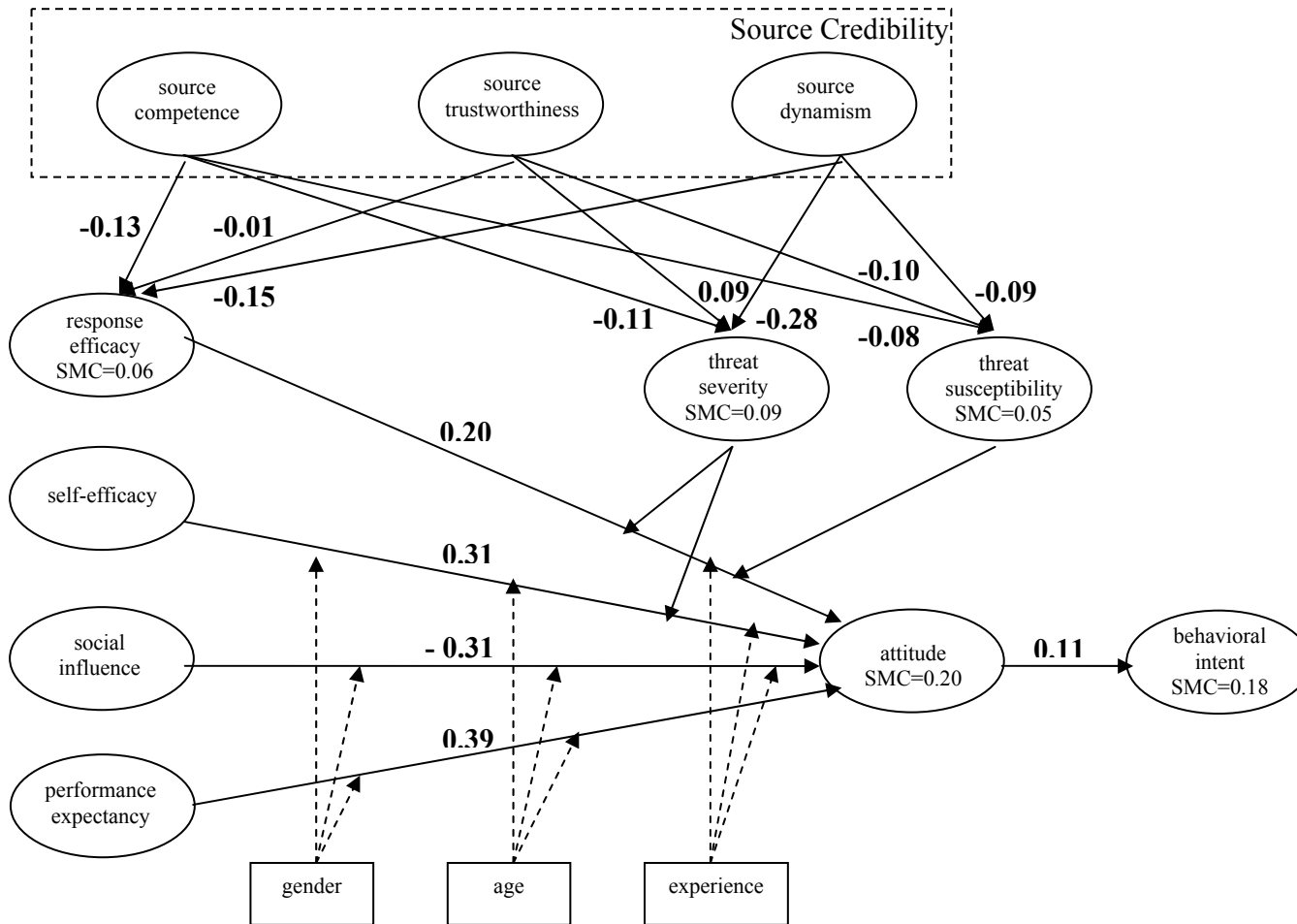


Figure 4.1

The Structural Model

To test the moderating affects of threat severity and threat susceptibility on the relationships between response efficacy and attitude, and that of self-efficacy and attitude, a multigroup analysis was performed. The analysis procedure involved the preliminary step of calculating a mean value for threat severity (3.93) and then grouping the respondents into two groups based on their responses to threat severity instrument items. Results indicated that 95 respondents scored a summated average of less than 3.93, whereas 120 respondents scored a summated average of greater than 3.93. The next step was to test the structural model using those responses of (a) the above mean group and (b) of the below mean group. An examination of overall goodness of fit statistics between the two structural model tests indicated a comparable level of overall fit (see Table 4.12); therefore, the two groups are the same.

Table 4.12 Comparison of Structural Models with High/Low Threat Severity

Threat Severity Response Group	χ^2	d.f.	RMSEA	NFI	NNFI	GFI	CFI
above mean	529.46	300	0.073	0.84	0.90	0.79	0.91
below mean	464.99	300	0.076	0.74	0.82	0.73	0.85

An examination of the paths was conducted next, with a differential in path t-value and coefficient values indicating a significance of the construct threat severity on the relationships between response efficacy and attitude, and self-efficacy and attitude (see Table 4.13). For the above mean (high-threat severity) responses, the t-values for response efficacy to attitude and self-efficacy to attitude were 1.96 and 2.81, respectively.

For the below mean (low-threat severity) responses, the t-values for response efficacy to attitude and self-efficacy to attitude were 1.17 and 5.13, respectively. These findings indicate that the path from response efficacy to attitude changed from significant to nonsignificant as the threat severity responses varied from high to low. This indicates a significant moderating effect for threat severity on the response efficacy to attitude relationship. As the threat severity responses varied from high to low, the significance of the relationship between self-efficacy and attitude increased from 2.81 to 5.13; thereby, indicating a significant moderating effect for threat severity on the relationship.

Table 4.13 Tests of Threat Severity as Moderating Variable

Path	High Threat Severity		Low Threat Severity	
	Estimate	t-value	Estimate	t-value
response efficacy → attitude	0.14	1.96	0.12	1.17
self-efficacy → attitude	0.25	2.81	0.50	5.13

The process was repeated for threat susceptibility resulting in a mean value of 3.69, to which 115 respondents scored above and 100 respondents scored below. As depicted in Table 4.14, the structural model was tested using those responses of (a) the above mean group and (b) of the below mean group. An examination of overall goodness of fit statistics between the two structural model tests indicated a comparable level of overall fit.

Table 4.14 Comparison of Structural Models with High/Low Threat Susceptibility

Threat Susceptibility Response Group	χ^2	d.f.	RMSEA	NFI	NNFI	GFI	CFI
above mean	511.65	300	0.077	0.81	0.88	0.76	0.90
below mean	442.09	300	0.071	0.78	0.88	0.74	0.90

An examination of the paths was conducted, with a differential in path t-value and coefficient values indicating a significance of the construct threat susceptibility on the relationships between response efficacy and attitude and that of self-efficacy and attitude. As shown in Table 4.15, for the above mean (high-threat susceptibility) responses, the t-values for response efficacy to attitude and self-efficacy to attitude were 2.28 and 0.09, respectively. For the below mean (low-threat susceptibility) responses, the t-values for response efficacy to attitude and self-efficacy to attitude were 1.71 and 5.25, respectively. These findings indicate that the path from response efficacy to attitude changed from significant to nonsignificant as the threat susceptibility responses varied from high to low. This indicates a significant moderating effect for threat susceptibility on the response efficacy to attitude relationship. Similarly, the path from self-efficacy to attitude changed from nonsignificant to significant as the threat susceptibility responses varied from high to low, which indicated a significant moderating effect for threat susceptibility on the self-efficacy to attitude relationship.

Table 4.15 Tests of Threat Susceptibility as Moderating Variable

Path	High Threat Susc.		Low Threat Susc.	
	Estimate	t-value	Estimate	t-value
response efficacy → attitude	0.19	2.28	0.15	1.71
self-efficacy → attitude	0.01	0.09	0.68	5.25

Interpretation

An examination of the model in Figure 4.1 indicates that 7 of the 18 hypotheses and subhypotheses investigated in this study were supported. This seemingly limited success in hypotheses support is somewhat exaggerated by the fact that 9 of the tested hypotheses were derived from a single construct, source credibility, which failed to form significant positive relationships with any of its prescribed dependent variables at a 0.05 level of significance. Additionally, social influence (t-value = -0.95) and performance efficacy (t-value = 1.09) had no significant impact on attitude. Results do indicate that self-efficacy (coefficient = 0.31, t-value = 4.85) had a higher level of explanatory power for attitude than did response efficacy (coefficient = 0.20, t-value = 3.10). Together the two constructs combine to explain approximately 20% of the variance in attitude. Attitude (coefficient = 0.11, t-value = 3.13) had a significant impact on behavioral intent, explaining about 18% of its variance.

As depicted in Table 4.16, hypothesis H1, which tested the positive relationship between attitude and behavioral intent, was supported. To be specific, attitude was found to have a positive effect on an end user's intent to adopt recommended individual computer security actions to ameliorate spyware. The supported H1 reinforces the

Theory of Planned Behavior (TPB), the Theory of Reasoned Action (TRA), and the Motivational Model (MM) in which attitude is regarded as the strongest determinant of behavioral intent (Venkatesh et al., 2003). Yang and Yoo (2004) also consider attitude to be a significant determinant of behavioral intent.

Table 4.16 Hypotheses and Model Estimation Components Testing Results

Hypotheses	Structural Relationship	Standard Parameter Estimate
H1	attitude has a <i>positive</i> influence on behavioral intent	supported* $\beta_1 = 0.11$
H2	social influence has a <i>positive</i> influence on attitude	not supported $\gamma_1 = -0.31$
H3	performance expectancy has a <i>positive</i> influence on attitude	not supported $\gamma_2 = 0.39$
H4	response efficacy has a <i>positive</i> influence on attitude	supported* $\beta_2 = 0.20$
H5	self-efficacy has a <i>positive</i> influence on attitude	supported* $\gamma_3 = 0.31$
H6a	a higher threat severity causes response efficacy to have a stronger positive influence on attitude	supported $\gamma_{4H} = 0.14$
	a lower threat severity causes response efficacy to have a weaker positive influence on attitude	supported $\gamma_{4L} = 0.12$

* $p < .01$

Table 4.16 (continued) Hypotheses and Model Estimation Components

Hypotheses	Structural Relationship	Standard Parameter Estimate
H6b	a higher threat severity causes self-efficacy to have a stronger positive influence on attitude	supported $\gamma_{5H} = 0.25$
	a lower threat severity causes self-efficacy to have a weaker positive influence on attitude	supported $\gamma_{5L} = 0.50$
H7a	a higher threat susceptibility causes response efficacy to have a stronger positive influence on attitude	supported $\gamma_{6H} = 0.19$
	a lower threat susceptibility causes response efficacy to have a weaker positive influence on attitude	supported $\gamma_{6L} = 0.15$
H7b	a higher threat susceptibility causes self-efficacy to have a stronger positive influence on attitude	supported $\gamma_{7H} = 0.01$
	a lower threat susceptibility causes self-efficacy to have a weaker positive influence on attitude	supported $\gamma_{7L} = 0.68$
H8a	source competence has a <i>positive</i> influence on threat severity	not supported $\gamma_8 = -0.11$
H8b	source competence has a <i>positive</i> influence on threat susceptibility	not supported $\gamma_9 = -0.08$
H8c	source competence has a <i>positive</i> influence on response efficacy	not supported $\gamma_{10} = -0.13$
H9a	source trustworthiness has a <i>positive</i> influence on threat severity	not supported $\gamma_{11} = 0.09$
H9b	source trustworthiness has a <i>positive</i> influence on threat susceptibility	not supported $\gamma_{12} = -0.10$

Table 4.16 (continued) Hypotheses and Model Estimation Components

Hypotheses	Structural Relationship	Standard Parameter Estimate
H9c	source trustworthiness has a <i>positive</i> influence on response efficacy	not supported $\gamma_{13} = -0.01$
H10a	source dynamism has a <i>positive</i> influence on threat severity	not supported $\gamma_{14} = -0.28$
H10b	source dynamism has a <i>positive</i> influence on threat susceptibility	not supported $\gamma_{15} = -0.09$
H10c	source dynamism has a <i>positive</i> influence on response efficacy	not supported $\gamma_{16} = -0.15$

Results indicate that H2 was not supported. Specifically, based on findings from this data set, there is no evidence that social influence will have a significant positive effect on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware. This finding contradicts previous theories such as TRA (Fishbein & Ajzen, 1975) in which social influence positively influences attitude (Hartwick & Barki, 1994). Yet, this finding is consistent with several studies that have determined social influence *not* to have an influential role in explaining attitude or behavioral intent (Davis et al., 1989). Therefore, given the lack of consensus among previous research outcomes concerning the role of social influence on attitude leading to behavioral intent, this particular outcome is unexpected, yet not entirely surprising. The rationale behind the unsupported hypothesis could lie in the context from which the hypothesized relationship was tested.

Threatening conditions, such as the prospect of spyware infestation, might temper the social exchange regarding anti-threat actions. Additionally, it is possible that subjects for this study were unable to differentiate between the source of the fear appeal and the source of the support for anti-spyware actions because they were one and the same.

Hypothesis H3 states that performance expectancy will have a significant positive effect on an end user's attitude toward the adoption of recommended individual computer security actions to ameliorate spyware. This hypothesis was not supported. Performance expectancy, a construct of the Unified Theory of Acceptance and Use of Technology (UTAUT), was included in the conceptual model as a means of accounting for perceived benefits that could be obtained from following recommended individual security actions. In this case that course of action was the use of anti-spyware software. The fact that the hypothesis was not supported could be a symptom of the context of the study.

Previous studies involving performance expectancy considered perceived benefits gained from the use of productivity-based technology such as online conferencing software or accounting information systems (Venkatesh et al., 2003). For example, as part of their longitudinal study toward the development of UTAUT, Venkatesh et al. (2003) investigated user expectations of performance from the use of a database application that could reference product industry standards. This application provided clear advantages to its users over previous methods such as product literature or online search engines. Not all technologies provide such obvious benefits (Warkentin et al., 2004). For some respondents, the context of this study could be perceived as one in which the primary objective of the recommended technology is not productivity.

Individual acts of security, such as anti-spyware usage, are simply a means of controlling their environments, or a means for maintaining a healthy technological baseline from which to employ productivity enhancing technologies. Therefore, performance benefits cannot be explicitly described.

The unexpected results concerning H3 may also indicate a discrepancy among users - those within highly volatile computing environments characterized by sluggish and unreliable system performance, and those within highly stable computing environments characterized by reliable, strong system performance. For those users within the highly stable computing environment, the performance gains expected from anti-threat technology, such as anti-spyware software, are negligible. Conversely, users operating within highly volatile computing environments may regard anti-spyware software as medicine for what ails their poor performing systems. Inconsistencies in perspectives such as these could explain why performance expectancy was not supported as a determinant of attitude.

Numerous studies (Stanley & Maddux, 1986; Witte et al., 1996) regard performance expectancy as closely related to response efficacy. This study attempts to differentiate between the two by defining performance expectancy as the degree to which an end user believes the adoption of anti-spyware actions will enhance his or her performance, and response efficacy as the degree to which an end user believes a recommended response will efficiently and effectively avert spyware. So, while performance expectancy considers the performance of the individual, response efficacy addresses the capability of the response task. Nevertheless, the two constructs do share a

similar underlying theme, the measure of perceived benefits based on the use of an anti-spyware product. This fact may explain the cross-loadings between the two factors.

Hypothesis H4 states that response efficacy will have a positive influence on attitude. Results indicate that this hypothesis is supported at a 0.05 level of significance with a beta value of 3.10. This finding reinforces Witte's (1992) Extended Parallel Process Model (EPPM) which articulates that an individual's beliefs in the ability of a recommended response to avert a threat will determine the manner in which he or she will address the threat. For anti-spyware software, potential users will consider what they know of its ability to thwart a spyware attack.

The fact that H5, which states the self-efficacy will have a positive influence on attitude, is supported also reinforces Witte's (1992) EPPM. EPPM regards self-efficacy together with response efficacy as two dimensions of efficacy. Self-efficacy plays a role in determining the manner in which an individual will address a threat. For anti-spyware protection, potential users of the software will consider their ability to follow through with the necessary steps in using the protection prior to its use.

The support for H6a and H6b is not surprising in that relationships between response efficacy and attitude and self-efficacy and attitude are not formed in isolation from threat. The supported hypotheses reinforce EPPM in that, once a decision has been made based on efficacy as to how to address a threat, perceptions of the severity of the threat will dictate the attitudinal intensity of the response. In other words, if a user perceives he or she is capable of using anti-spyware software and that the software is effective in fighting off a spyware assault, his or her perception of the severity of the

spyware menace will help shape his or her attitude regarding the response. For example, it could be expected that users that perceive the threat to be of great severity will have a better disposition for using the software than those that perceive the threat to be of low severity.

Findings also suggest the moderating effect of threat susceptibility on the relationships between response efficacy and attitude and self-efficacy and attitude is significant. The supported H7a suggests that perceptions of the susceptibility of the spyware threat moderate the relationship between response efficacy and attitude, while the supported H7b suggests that this moderating effect also holds for the relationship between self-efficacy and attitude.

Finally, hypotheses H8, H9, and H10, each with three subhypotheses, are all unsupported based on the results obtained from this study's data set. These hypotheses are intended to test three dimensions of source credibility on the outcome variables of perceived threat severity, perceived threat susceptibility, and response efficacy. The three dimensions of source credibility are source competence, source trustworthiness, and source dynamism. The fact that none of the proposed hypotheses are supported contradicts previous research. Specifically, the unsupported relationships of the three dimensions of source credibility with threat severity and threat susceptibility defy the contentions of Hewgill and Miller (1965), in which they claim perceptions of threat to intensify as the credibility of the source increases.

There are many possible explanations why the dimensions of source credibility failed to relate significantly to their anticipated constructs. Previous research has

demonstrated that when individuals perceive the source of a threatening message to be of high credibility, they demonstrate significant changes in attitude and behavior related to the message. However, when exposed to messages in which they perceive the source to be of low credibility, their reactions are not different from those unexposed to the message. Perhaps the absence of significant findings concerning source credibility in this study can be attributed to the intentional use of an unknown source, one that does not engender preconceived notions of credibility among respondents. The fear appeal treatment was purposely designed to be neutral, so that the respondents would form their own opinions as to the actor's credibility without any preconceived ideas.

Post Hoc Analysis

According to Joreskog and Sorborn (1993), structural models may be respecified on the basis of the fit indices resulting from tests of the original model. However, any new causal relationships included in the respecification must be justified by theory. The following sections address the respecification of the structural model based on theoretical support.

Respecification of the Structural Model

In that the overall fit statistics of the structural model indicate only an adequate fit of the model to the data (RMSEA = 0.068, NFI = 0.87, NNFI = 0.91, GFI = 0.83, and CFI = 0.92), a post hoc analysis of the model was considered. The analysis resulted in a respecification of the model in which a single theoretically justified path was included, thereby improving the fit indices (Table 4.17).

As stated earlier, performance expectancy was developed from the synthesis of constructs from several competing models, including perceived usefulness (Davis, 1989; Davis et al., 1989) and outcome expectations (Compeau & Higgins, 1995b; Compeau et al., 1999). Response efficacy, while distinguished from performance expectancy in this study, is frequently regarded as a similar factor (Stanley & Maddux, 1986; Witte et al., 1996). As such, response efficacy could be expected to behave similarly in the presence of certain variables, specifically social influence. Venkatesh and Davis (2000) cite social influence as a direct determinant of perceived usefulness; thereby implying that social influence will form a similar relationship with response efficacy. Therefore, as suggested in the LISREL output modification indices and supported in theory, a path was added between social influence and response efficacy. Based on the inclusion of this path in the model, the RMSEA improved from 0.068 to 0.065. Other key indicators of model fit include NFI = 0.87, NNFI = 0.92, GFI = 0.84, and CFI = 0.93.

Table 4.17 Model Respecification Process for Structural Model

Step	Changes Made From Previous Step	χ^2	d.f.	RMSEA	NFI	NNFI	GFI	CFI
	proposed model	593	300	0.068	0.87	0.91	0.83	0.92
1	add social influence → response efficacy	572	299	0.065	0.87	0.92	0.84	0.93

Table 4.18 depicts the results of the respecified structural model analysis in terms of paths. The path from response efficacy to attitude (t-value = 3.02), the path from attitude to behavioral intent (t-value = 3.14), and the path from self-efficacy to attitude (t-

value = 4.83) remained significant at better than a 0.05 level of significance. The included path of social influence to response efficacy was significant ($p < 0.01$) with a t-value of 4.26. All other paths remained nonsignificant.

Table 4.18 Standardized Path Estimates for Respecified Structural Model

Path	Estimate	t-value	p-value
response efficacy → attitude	0.21	3.02	< 0.01
attitude → behavioral intent	0.11	3.14	< 0.01
source competence → response efficacy	-0.09	-0.84	n.s.
source trustworthiness → response efficacy	-0.10	-0.97	n.s.
source dynamism → response efficacy	-0.04	-0.48	n.s.
source competence → threat severity	-0.11	-0.98	n.s.
source trustworthiness → threat severity	0.09	0.88	n.s.
source dynamism → threat severity	-0.28	-3.09	n.s.
source competence → threat susceptibility	-0.08	-0.76	n.s.
source trustworthiness → threat susceptibility	-0.10	-0.95	n.s.
source dynamism → threat susceptibility	-0.09	-0.98	n.s.
self-efficacy → attitude	0.31	4.84	< 0.01
social influence → attitude	-0.32	-0.98	n.s.
performance expectancy → attitude	0.39	1.12	n.s.
social influence → response efficacy	0.31	4.26	< 0.01

$\chi^2 = 572.30$ (d.f. = 299)

RMSEA = 0.065, NFI = 0.87, NNFI = 0.92, GFI = 0.84, and CFI = 0.93

As with the proposed model, a comparison of two respecified models, one with high threat severity responses and one with low-threat severity responses was performed to determine if threat severity had a moderating effect on response efficacy and self-efficacy. The examination of overall goodness of fit statistics between the two structural

model tests indicated a comparable level of overall fit. This comparison and its resultant fit statistics are presented in Table 4.19.

Table 4.19 Comparison of Respecified Structural Models with High/Low Threat Severity

Threat Severity Response Group	χ^2	d.f.	RMSEA	NFI	NNFI	GFI	CFI
above mean	419.75	299	0.058	0.84	0.93	0.79	0.94
below mean	392.44	299	0.063	0.74	0.85	0.74	0.85

A path analysis of the two structural model tests revealed results similar to those of the proposed model. As indicated in Table 4.20, the changes in t-values for the relationship between response efficacy and attitude and that of self-efficacy and attitude suggest that threat severity moderates the relationships.

Table 4.20 Tests of Threat Severity as Moderating Variable

Path	High Threat Severity		Low Threat Severity	
	Estimate	t-value	Estimate	t-value
response efficacy → attitude	0.15	1.96	0.13	1.24
self-efficacy → attitude	0.26	2.54	0.50	5.12

A comparison of high-threat susceptibility and low-threat susceptibility responses for the respecified model resulted in findings similar to those of the proposed model.

Table 4.21 presents the overall fit statistics from comparisons of the respecified structural models under conditions of both high and low threat susceptibility. The fit statistics

suggest the models to be comparable. As indicated in Table 4.22, the changes in t-values for the relationship between response efficacy and attitude and that of self-efficacy and attitude suggest that threat susceptibility moderates the relationships.

Table 4.21 Comparison of Respecified Structural Models with High/Low Threat Susceptibility

Threat Susceptibility Response Group	χ^2	d.f.	RMSEA	NFI	NNFI	GFI	CFI
above mean	491.58	299	0.074	0.82	0.89	0.77	0.91
below mean	441.29	299	0.071	0.78	0.88	0.74	0.90

Table 4.22 Tests of Threat Susceptibility as Moderating Variable

Path	High Threat Susc.		Low Threat Susc.	
	Estimate	t-value	Estimate	t-value
response efficacy → attitude	0.19	2.07	0.16	1.81
self-efficacy → attitude	0.01	0.08	0.68	5.20

Interpretation

As was the case with the original proposed structural model, the final structural model analysis indicated 7 of the original 18 hypotheses were supported. The final structural model, however, provided for a greater degree of predictive power for response efficacy. As illustrated in Figure 4.2, 14.7% of the variance in response efficacy was explained. Also, attitude was able to explain 18.4% of the variance in behavioral intent and 20.4% of the variance in attitude. As opposed to response efficacy, self-efficacy

remained a stronger predictor of attitude with a coefficient of .31. Figure 4.3 illustrates the respecified model, showing only those paths that are significant.

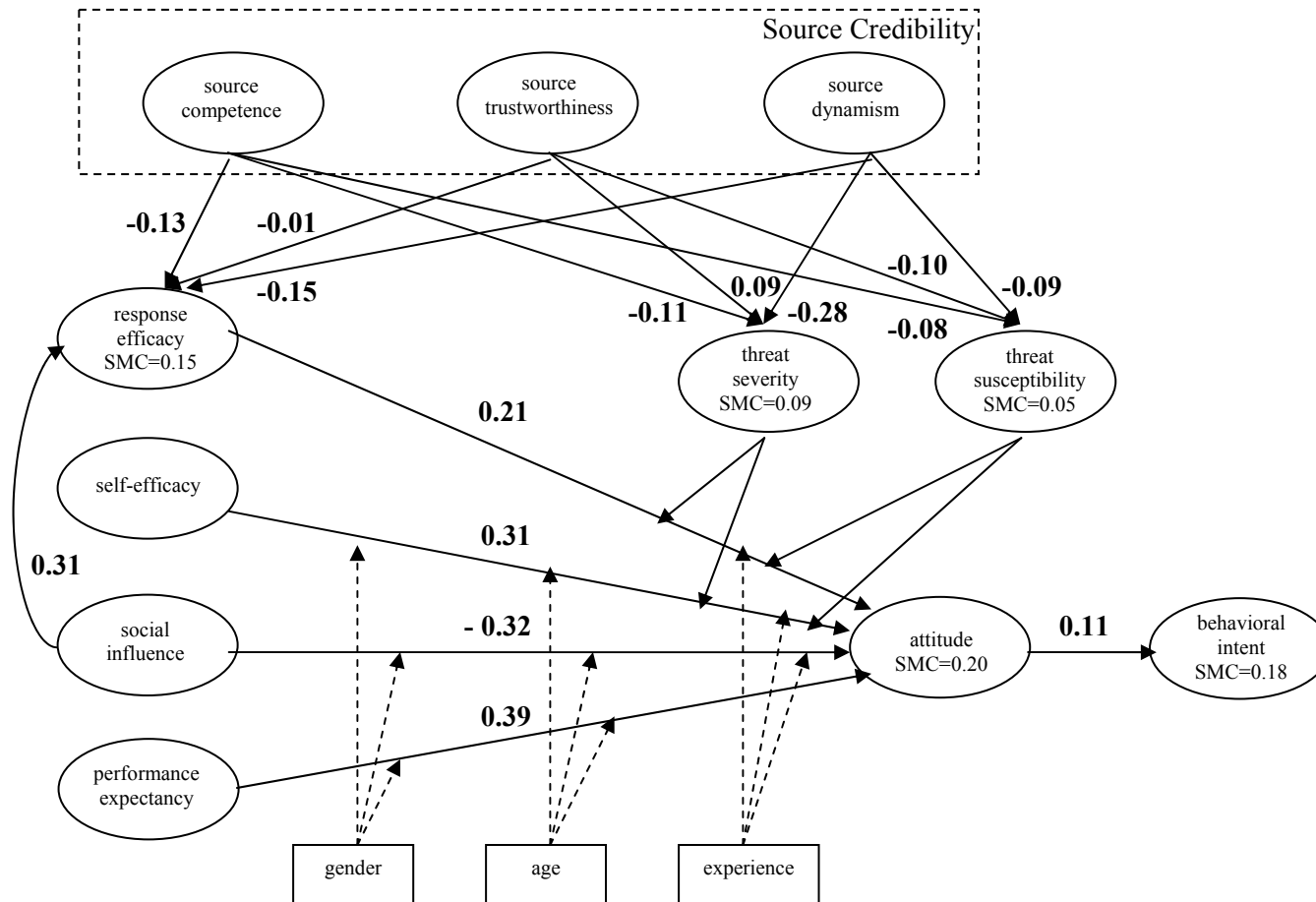


Figure 4.2
The Respecified Structural Model

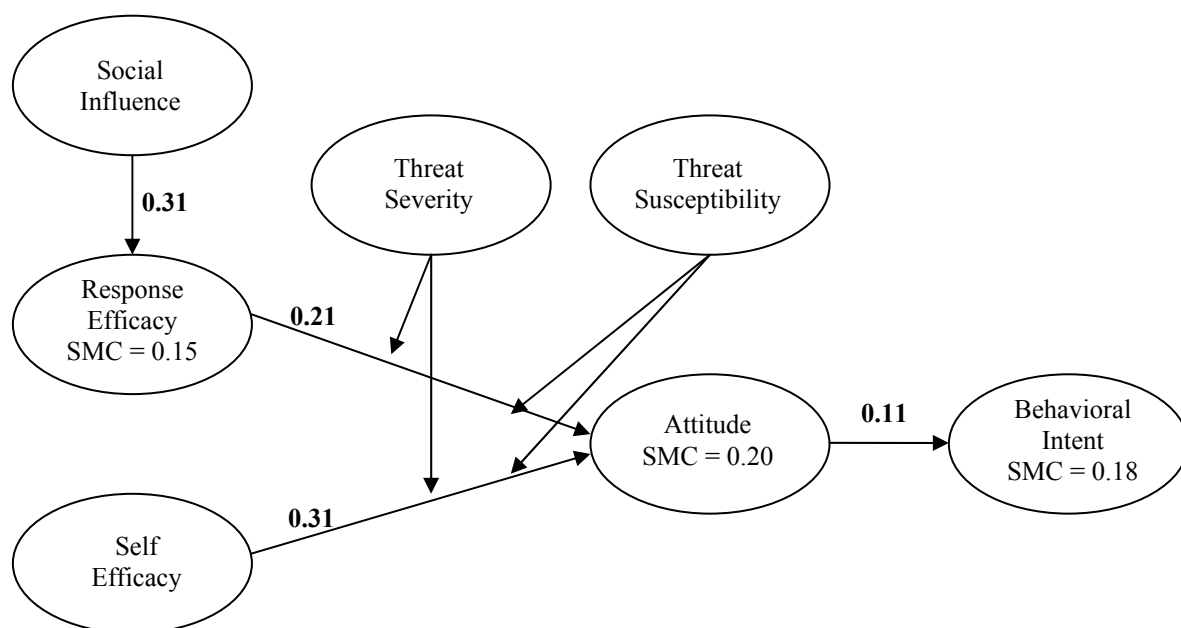


Figure 4.3

Structural Model with Only Significant Paths

Summary

This chapter discussed the EFA results of the preliminary investigation phase as well as the statistical analyses and results of the primary investigation phase of the dissertation. Included in the primary phase analyses were internal and external validity tests involving randomly assigned groups of participants as dictated by the Solomon four-group design. Next, tests of the measurement model and structural model were made using SEM. Finally, a post hoc analysis was conducted based on results of the

modification index and IS theory. The final results indicate support for seven of the original hypotheses and support the relationship of social influence as a determinant of response efficacy. As with the original structural model, the respecified model garnered adequate fit with the data.

The following chapter provides implications of this research in terms of both academia and practice and discusses limitations of this research. The chapter concludes with future research opportunities based on omissions and limitations of this study.

CHAPTER V

DISCUSSION AND CONCLUSION

The research question to be answered by this dissertation was: How do fear appeals modify end users' attitudes and behavioral intentions associated with recommended individual computer security actions? While pursuing an answer to this question, a two-phase examination was adopted that involved two distinct data collection and analysis procedures.

The first phase, or preliminary phase, involved tests to ensure that the instrument, treatment, and experimental procedure were appropriate, accurate, and reliable for the purposes of this research. These preliminary tests were based on results obtained from a sample of 200 undergraduate students at Mississippi State University and included: (a) content validity tests of both the instrument and the experimental treatment; (b) construct validity and reliability tests, including convergent and discriminant validity tests of the scale items used to measure the underlying constructs of the conceptual model; and (c) a pilot study to ascertain the proper working condition of the experimental procedure.

The second phase, or primary phase, of investigation involved the development and testing of a conceptual model representing an infusion of theories based on prior research in Social Psychology and Information Systems (IS), namely the Extended Parallel Process Model (EPPM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). Based on a Solomon four-group research design involving data

obtained from 341 faculty, staff, and students from Mississippi State University, analysis of variance (ANOVA) tests were first conducted to control for issues of internal and external validity that could jeopardize the research. The findings of the ANOVA analysis suggested that at least one outcome variable, attitude, was significantly altered due to the presence of a fear-inducing arguments. Additionally, the application of a pretest did not significantly alter the posttest responses. Next, a Structural Equation Modeling approach to data analysis was used to perform tests of both the measurement and structural models of this research.

The outcomes of tests involved in this study indicate support for 7 of the 18 hypotheses associated with the research model. And, in answering the research question (How do fear appeals modify end users' attitudes and behavioral intentions associated with recommended individual computer security actions?) the resulting model of this study provides 20% and 18% of the explained variance in attitude and behavioral intent, respectively. The focus of this chapter is a discussion of the implications of the study, both for academia and industry. The chapter concludes with potential limitations of the study and directions for future research.

Implications for IS Theory

This study makes a contribution to the field of IS by taking a well-established theory for explaining human reaction to fear-inducing messages from the domain of Social Psychology and introducing it to the domain of IS. EPPM represents a culmination of years of research and improvements to fear appeal theory, and its impact within the realm of IS research is promising. The results of this study demonstrate that

EPPM translates well to the field of IS security. Self-efficacy and response efficacy have a significant direct impact on attitude toward individual computer security actions, and attitude has a significant direct influence on behavioral intent to perform those same actions. Additionally, the relationships between self-efficacy and attitude and that between response efficacy and attitude are governed by the perceptions of threat severity and threat susceptibility.

An established theory for explaining the acceptance and use of new technology is UTAUT. UTAUT is the most recent and powerful model for predicting user behavior within the domain of information technology (IT) acceptance. However, UTAUT is limited in its ability to explain the acceptance and use of security technology because it does not include the concept of threat. As this study shows, it is the perception of threat that motivates action for protection. By integrating EPPM with UTAUT, this study presents a new model, one which can provide more predictive power for technology acceptance under conditions of duress caused by threatening conditions.

Beyond the addition of the element of threat to UTAUT, this study extends UTAUT through the inclusion of attitude as a direct antecedent of behavioral intent. Originally tested as part of UTUAT, attitude was ultimately dropped from that theory for reasons of parsimony. Guided by the theoretical underpinnings of EPPM, attitude was included in this study's conceptual model and found to play a significant role in predicting behavioral intent to perform individual acts of computer security. While the debate among IS scholars over the role of attitude as a determinant of behavioral intent remains unresolved, this study supports its inclusion.

The fact that performance expectancy and social influence were not found as significant determinants of attitude has implications for IS theory. While these factors have been included in previous models predicting user attitudes or intentions to use new technology or systems, they apparently play a significantly lesser role for end users in fear arousing situations. For instance, in developing UTAUT, Venkatesh et al. (2003) promote performance expectancy as a construct derived from a synthesis of various factors from previous literature in which the goal was to gauge productivity, promotion, rewards, performance gains, and expected outcome benefits. When considered within the context of expected performance attributed to the use of information security devices or procedures, perceptions of what constitutes “performance” are divided, and this division suggests further review of the applicability of the construct. Also, because empirical evidence from previous research concerning the impact of social influence on attitude is inconsistent, the fact that it is found nonsignificant in this study only contributes to the debate.

Based on the findings of this study and the discussion presented above, it could be argued that the domain of technology acceptance is not uniform and that findings from research in this area may not be universally applicable. Rather, research efforts within this area should identify and clearly state the conditions under which the investigations are to proceed. For instance, research involving technologies that serve to provide clear benefits to all who use them should be distinguished from those that involve technologies that serve only to reconstitute “normal” conditions. This study may serve as a point of origin for new discussions along these lines.

Implications for IS Practice

An issue faced by nearly all IT managers is how to motivate their end user constituents to follow policy and procedures for securing their respective computing interests. While numerous researchers have pointed to the use of emotional messages to inspire end users to practice safe computing, no study has been performed that attempts to conceptualize and test a model for predicting how users will respond to fear-inspiring communications. This dissertation makes a contribution in this respect and provides IT managers with insight for tailoring their fear appeals for maximum effectiveness.

The results of this study support the use of fear-inducing arguments as an effective way to influence end user attitudes and intentions to carry out recommended individual security actions. However, indications are that these messages inspire different outcomes for different users based on their perceptions of efficacy and threat. Messages warning of new threats and advising a plan of action to counter the threat will inspire some users to take appropriate action. For others, their reaction may be the opposite of what is suggested, thereby leaving some vulnerabilities unaddressed and exposing the entire firm to potential harm. Therefore, a holistic approach to this form of communication is not advised. Rather, to effectively wield fear as a motivator, IT managers must devise a strategy in which end users are exposed to fear appeals with language suitable to their efficacy level.

As the results of this study demonstrate, a predictor of how an end user will react to a fear appeal is his or her perceived self-efficacy. The fact that the study results suggest self-efficacy has a more powerful influence than response efficacy on attitude

suggests IT managers should focus a larger portion of their energies on developing the self-efficacy levels of their end users through training initiatives and other enhancement activities. As their self-efficacy levels increase, their attitudes and intentions for practicing more difficult tasks in high threat situations also increase. Perhaps measures of end users self-efficacy should be integrated into enterprise-wide training or policy awareness initiatives. These measures could provide managers with an index from which to classify users for efficient and effective communication. Based on this end user self-efficacy taxonomy, IT managers could employ a hybrid approach to communication in which messages are constructed for different end user audiences based on their self-efficacy classification. For those users with low self-efficacy, the messages should articulate a simple threat aversion procedure; while promoting the users' ability to perform the task. Conversely, high self-efficacy users may be provided messages that highlight the threat component in order to inspire action on their part.

This study also aids the practice of IS management by exposing the inherent dangers of user autonomy in the struggle to secure corporate and individual level resources. As the results of this study suggest, end users are not consistent in their attitudes and behavioral intent to comply with recommendations to protect their informational assets. As a result, decentralized IT governance environments, which place a significant portion of decision making and system management in the hands of the end user, are riddled with opportunities for vulnerability exploitation.

Not all firms are able to pattern their IT governance structure based on the requirements of secure computing. In fact, the governance of IT commonly mirrors that

of the organization's other business units. However, for those firms that are able, a centralized approach to computer security management may be more appropriate. Missed opportunities to capitalize on the localized proficiencies associated with a decentralized structure, such as response speed to user needs and customization of IT solutions, may be overshadowed by gains in information assurance.

Limitations

As with all research, this study has limitations; however, it is hoped that these shortcomings will be addressed as opportunities for future research. Probably the two most significant limitations are the result of the researcher's attempt to develop and test a parsimonious model within a reasonable time frame. Established theory, based on previous research, provided guidance and justification for the proposed model. However, the sheer number of possible antecedents of attitude, behavioral intent or behavior described in the literature make including all of them impractical. For this reason, constructs such as propensity to trust and propensity to fear were not considered.

While the trustworthiness of the source of a fear appeal is positioned as one of three dimensions of the Leathers Personal Credibility Scale (Leathers, 1992), the audience's propensity to trust was not accounted for. Considered an antecedent of trust in dyadic and group relationships, trust is often characterized and measured as a perception an individual has in others as to their ability, integrity, and benevolence. Trust is also an inherent characteristic of an individual, a quality that predicates the degree to which the individual will be influenced through trust-building exercises. Although absent from this study, an individual's inclination to trust others should be included in future

research regarding the effectiveness of fear appeals involving computer security. No doubt, the ambiguity associated with threats to information assurance plays a significant role in shaping the attitudes and intentions of individuals in performing security actions. If these individuals are not inclined to trust the sources that issue warnings or provide guidance, it is likely that they will not place much value in them.

Behavior is an important dependent variable in the proposed model but was not tested in the current research. Measures of behavior would require self-reported or third party data over a period of time involving the same respondents. Unfortunately, restrictions on the respondents' schedules prohibited a longitudinal research design. Additionally, it was presumed that during the time period between initial testing for behavior and subsequent measures of behavior, exposure to communicated messages of computer security threats and aversion techniques could not be controlled.

Another limitation of this study concerns the respecification of the model. A respecified model should be tested. In lieu of new data, one common approach to this task is a split sample analysis. Using a split sample analysis, the researcher splits the data sample set in half, uses the first half to test the proposed model, respecifies the model, and then uses the second half of the data sample to test the respecified model. Unfortunately, the sample collected in this research was not large enough to perform this validation.

Another limitation in this study is found in its use of faculty, staff, and students from Mississippi State University. While fulfilling the role desired by this study, that of end users having stake in the protection of computer technology, the faculty, staff, and

students of the university operate in an environment unlike that found in the corporate world. University settings are inherently insecure. As a result, the attitudes and behavioral intentions of the employees and students toward acts of security could be skewed to some degree by the “open” nature of university computing environments. While numerous previous studies concerning computer security and information assurance have involved higher education employees or students (Warkentin et al., 2004; Aytes & Connolly, 2004), the use of this convenience sample represents a threat to the generalizability of the findings.

A limitation of this research is also found in the fact that 83% of the respondents were between the ages of 18 and 29. This is not an accurate reflection of a cross-section of end users from Mississippi State University, and may limit the generalizability of the results. However, in a recent article published in the *Journal of Organizational and End User Computing*, Knight and Pearson (2005) find no differences among the various age ranges regarding computer behavior in the workplace. Considering that behavior is determined by attitude and behavioral intentions, the two outcome variables of this study, the exact ramifications of a limited age spectrum on the generalizability of the findings remains unclear.

Finally, it should be mentioned that source credibility is a heavily researched and well-documented topic. Unfortunately, the many dimensions and facets involved in identifying and measuring perceptions of credibility require a minimalist approach to its incorporation into the present research. To this end, dimensions such as source expertise, persistence, timing and message variables such as discrepancy, source-message

incongruity, and evidence were omitted from this investigation. While these aspects of credibility are important, parsimony of the conceptual model dictated their absence.

Future Research

The findings of this dissertation may prove valuable to both academicians and practitioners alike. However, there are many areas in which new research can either address limitations of this work or advance ideas derived from the results of this study. For instance, how do the innate propensities for fear and trust influence an individual's perceptions of efficacy and threat leading to outcome variables such as attitude and behavioral intent? It stands to reason that for those individuals that have a high tolerance for fear, the intensity of the threat must be greater than for those of lesser tolerance if action is to be taken. Empirical work in this direction would provide important insight for IS managers attempting to appropriately tailor their fear appeals to entice favorable responses from their constituents.

Another important direction of future study would be the investigation of fear appeal influence among different cultures within the context of security compliance. By leveraging cultural diversity, many firms are able to find benefits such as new idea generation and unique problem solving methods. However, diversity within the community may also degrade trust levels among its members (Gefen, Rose, Warkentin, & Pavlou, 2005). Do initiatives involving fear-inducing persuasive messages invoke the same outcomes for all cultures, or do cultural differences, such as those found in individualistic or collectivistic societies, moderate reactions to the fear appeals? Conceptual and empirical efforts in this direction would have practical value for those IS

managers attempting to gain consistent responses toward compliance efforts across all representative cultures of their firm.

The present study did not find significant relationships between the dimensions of source credibility and perceptions of threat severity, threat significance or response efficacy. This is counter to Hewgill and Miller's (1965) contention that the credibility of the fear appeal source will have an impact on the degree to which the appeal is able to affect change in end user attitudes and behavioral intentions. This study used the Leathers Personal Credibility Scale (Leathers, 1992) scale for measuring source credibility. Future research utilizing a different scale for measuring source credibility is needed to determine if source credibility is in fact not a significant determinant.

Finally, future research endeavors should examine the persistency of fear appeal effectiveness. How persistent are the effects of a fear appeal, and what factors serve to facilitate the degradation of fear appeal effectiveness? Do more frightening fear appeals influence end users for a longer period of time than less frightening fear appeals? At what point do end users draw upon their experiences and third party observations and become conditioned to this form of communication? These are research opportunities that could leverage the work of scholars in the fields of Social Psychology, Management, and Marketing, among others, to explore these questions within the context of human/computer interaction, organizational communications, or other psychosociometric investigations of end point security.

REFERENCES

- Ajzen, I. (1988). Attitude structure and behavior relations. In A. R. Partkanis, S. T. Berckler & A. G. Greenwald (Eds.), *Attitude structure and function*. Hillsdale, NJ: Erlbaum.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.
- Al-Gahtani, S. S., & King, M. (1999). Attitudes, satisfaction and usage: Factors contributing to each in the acceptance of information technology. *Behavior and Information Technology*, 18(4), 277-297.
- Alreck, P. A., & Settle, R. B. (1995). *The survey research handbook* (2nd ed.). Chicago: Irwin.
- 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.
- Associates, N. (2004). *Network Associates introduces McAfee antispyware - essential protection against spyware for consumers*. Retrieved March, 2005, from <http://www.net-security.org/press.php?id=1973>
- Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational & End User Computing*, 16(3), 22-40.
- Babbie, E. (2004). *The practice of social research* (10th ed.). Belmont, CA: Wadsworth/Thomson Learning.
- Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, 37(2), 122-147.
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice Hall.
- Bannister, B. D. (1986). Performance outcome feedback and attributional feedback: Interactive effects on recipient responses. *Journal of Applied Psychology*, 71, 203-210.
- Beck, K. H., & Frankel, A. (1981). A conceptualization of threat communications and protective health behavior. *Social Psychology Quarterly*, 44, 204-217.

- Bentler, P. M., & Bonnett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, 88(3), 588-606.
- Berlo, D. K., & Lemert, J. B. (1961, December). *An empirical test of a general construct of credibility*. Paper presented at the SAA Conference, New York, NY.
- Bhattacharjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, 25(3), 351-370.
- Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1-16.
- Campbell, D., & Stanley, J. (1963). *Experimental and quasi-experimental designs for research*. Chicago: Rand McNally.
- Cannon, W. B. (1915). *Bodily changes in pain, hunger, fear, and rage*. New York: Appleton.
- Casey, M. K. (1995, November). *Fatalism and the modification of the extended parallel process model*. Paper presented at the Speech Communication Association, San Antonio, Texas.
- Cates, J. A., Dian, D. A., & Schnepf, G. W. (2003). Use of protection motivation theory to assess fear of crime in rural areas. *Psychology, Crime & Law*, 9(3), 225.
- Chaiken, S. (1979). Communicator physical attractiveness and persuasion. *Journal of Personality and Social Psychology*, 37(8), 1387-1397.
- 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.
- Colvin, C. A., & Goh, A. (2005). Validation of the technology acceptance model for police. *Journal of Criminal Justice*, 33(1), 89-95.
- Compeau, D., & Higgins, C. A. (1995a). Application of social cognitive theory to training for computer skills. *Information Systems Research*, 6(2), 118-143.
- Compeau, D., & Higgins, C. A. (1995b). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 19, 189-211.

- Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly*, 23(2), 14-158.
- Cook, T. D., & Campbell, D. T. (1979). *Quasi experimentation: Design and analytical issues for field settings*. Chicago: Rand McNally.
- Crano, W. D. (1970). Effect of sex, response order, and expertise in conformity: A dispositional approach. *Sociometry*, 33, 239-252.
- Crisci, R., & Kassinove, H. (1973). Effect of perceived expertise, strength of advice, and environmental setting on parental compliance. *Journal of Social Psychology*, 89, 245-250.
- Cybercrime: Expansive and expensive. (2005, March). *Baseline*, 39.
- Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science*, 32(5), 554-571.
- Daft, R. L., Lengel, R. H., & Trevino, L. (1987). Message equivocality, media selection, and manager performance. *MIS Quarterly*, 11(3), 355-366.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 318-340.
- Davis, F. D. (1993). User acceptance of information technology: Systems characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, 38, 475-487.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35, 982-1003.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology*, 22(14), 1111-1132.
- Deem, R. (2004). The knowledge worker, the manager-academic and the contemporary U.K. university: New and old forms of public management. *Financial Accountability and Management*, 20(2), 107-128.
- Dejong, W., & Wallack, L. (1999). A critical perspective on the drug czar's antidrug media campaign. *Journal of Health Communication*, 4(2), 155-160.

- Delone, W. H., & McLean, E. R. (1992). Information systems success: The quest of the dependent variable. *Information Systems Research*, 3, 60-95.
- Dennis, A. R., & Kinney, S. T. (1998). Testing media richness theory in the new media: The effects of cues, feedback, and task equivocality. *Information Systems Research*, 9(3), 256-274.
- Dillard, J. P. (1994). Rethinking the study of fear appeals: An emotional perspective. *Communication Theory*, 4, 295-323.
- Dillard, J. P., Plotnick, C. A., Godbold, L. C., Freimuth, V. S., & Edgar, T. (1996). The multiple affective outcomes of AIDS PSAs: Fear appeals do more than scare people. *Communications Research*.
- Druker, P. (1959). *The landmarks of tomorrow*. New York: Harper and Row.
- Eagly, A. H., & Chaiken, S. (1975). An attribution analysis of the effect of communicator characteristics on opinion change: The case of communicator attractiveness. *Journal of Personality and Social Psychology*, 32(1), 136-144.
- Etezadi-Amoli, J., & Farhoomand, A. (1996). A structural model of end-user computing satisfaction and user performance. *Information and Management*, 30(2), 65-73.
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior*. Reading, MA: Addison-Wesley.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equations with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50.
- Fowler, F. J. (1984). *Survey research methods*. Beverly Hills, CA: Sage.
- Freud, S. (1936). *The problem of anxiety*. New York: W.W. Norton.
- Fry, R. B., & Prentice-Dunn, S. (2005). Effects of coping information and value affirmation on responses to a perceived health threat. *Health Communication*, 17(2), 133-147.
- Gangloff, B. (1981). Communicator credibility, message credibility, and dissuasion: Experiments in a suburban setting. *Bulletin de Psychologie*, 34, 748-753.
- Gefen, D., Rose, G. M., Warkentin, M., & Pavlou, P. A. (2005). Cultural diversity and trust in it adoption: A comparison of potential e-voters in the USA and South Africa. *Journal of Global Information Management*, 13(1), 55-79.

- Gefen, D., Straub, D., & Boudreau, M. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communications of AIS*, 7(7), 1-78.
- Goodhue, D. (1988). Is attitudes: Toward theoretical and definition clarity. *Data Base*, 19(3/4), 6-15.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). 2004 CSI/FBI computer crime and security survey (pp. 1-16): Computer Security Institute.
- Grunfeld, E. A. (2004). What influences university students' intentions to practice safe sun exposure behaviors? *Journal of Adolescent Health*, 35(6), 486-492.
- Gutek, B. A., & Winter, S. J. (1990). Computer use, control over computers, and job satisfaction. In S. Oskamp & S. Spacapan (Eds.), *People's reactions to technology, the Claremont symposium on applied social psychology* (Vol. 4). Newbury Park, CA: Sage.
- Harrison, D. A., Jr., P. P. M., & Riemenschneider, C. K. (1997). Executive decisions about adoption of information technology in small business: Theory and empirical tests. *Information Systems Research*, 8(2), 171-195.
- Hartwick, J., & Barki, H. (1994). Explaining the role of user participation in information system use. *Management Science*, 40(4), 440-465.
- Hewgill, M. A., & Miller, G. (1965). Source credibility and response to fear-arousing communications. *Speech Monographs*, 32(2), 95-101.
- Hoog, N. d., Stroebe, W., & Wit, J. B. F. d. (2005). The impact of fear appeals on processing and acceptance of action recommendations. *Personality and Social Psychology Bulletin*, 31(1), 24-33.
- Horai, J., Naccari, N., & Fatoullah, E. (1974). The effects of expertise and physical attractiveness upon opinion agreement and liking. *Sociometry*, 37, 601-606.
- Hovland, C., Janis, I. L., & Kelly, H. (1953). *Communication and persuasion*. New Haven, CT: Yale University Press.
- Hovland, C., & Weiss, W. (1951). The influence of source credibility on communication effectiveness. *Public Opinion Quarterly*, 15, 635-650.
- Igbaria, M. (1990). End-user computing effectiveness: A structural equation model. *OMEGA International Journal of Management Science*, 18(6), 637-652.

- Igbaria, M., & Chakrabarti, A. (1990). Computer anxiety and attitudes towards microcomputer use. *Behavior and Information Technology, 9*, 229-241.
- Izard, C. E. (1977). *Human emotions*. New York: Plenum Press.
- Janis, I. L. (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 3, pp. 166-225). New York: Academic Press.
- Janis, I. L., & Feshbach, S. (1953). Effects of fear-arousing communications. *Journal of Abnormal and Social Psychology, 48*, 78-92.
- Johnson, H. H., & Izzett, R. (1969). Relationship between authoritarianism and attitude change as a function of source credibility and type of communication. *Journal of Personality and Social Psychology, 13*, 317-321.
- Johnson, H. H., Torvicia, J., & Poprick, M. (1968). Effects of source credibility on the relationship between authoritarianism and attitude change. *Journal of Personality and Social Psychology, 9*, 179-183.
- Joreskog, K. G., & Sorbom, D. (1993). *LISREL 8: Structural equation modeling with the SIMPLIS command language*. Chicago, IL: Scientific Software International.
- Kavanagh, D. J., & Bower, G. H. (1985). Mood and self-efficacy: Impact of joy and sadness on perceived capabilities. *Cognitive Theory and Research., 9*, 507-525.
- Keat, T. K., & Mohan, A. (2004). Integration of TAM based electronic commerce models for trust. *Journal of American Academy of Business, Cambridge, 5*(1/2), 404-410.
- Kelloway, E. K. (1996). Common practices in structural equation modeling. In C. L. Cooper & I. Robertson (Eds.), *International review of industrial and organizational psychology* (pp. 141-180). Chichester, UK: John Wiley and Sons.
- Kelloway, E. K. (1998). *Using LISREL for structural equation modeling*. Thousand Oaks, CA: Sage.
- Kelman, H., & Hovland, C. (1953). "Reinstatement" Of the communicator in delayed measurement of opinion. *Journal of Abnormal and Social Psychology, 48*, 327-335.
- Kenton, S. B. (1989). Speaker credibility in persuasive business communication: A model which explains gender differences. *Journal of Business Communication, 26*(2), 143-157.

- Knight, M. B., & Pearson, J. M. (2005). The changing demographics: The diminishing role of age and gender in computer usage. *Journal of Organizational and End User Computing, 17*(4), 49-65.
- Landesman, M. (2005). Spyware stoppers. *PC World, 23*(4), 68-75.
- Lang, P. J. (1984). Cognition in emotion: Concept and action. In C. E. Izard, J. Kagan & R. B. Zajonc (Eds.), *Emotions, cognition, and behavior* (pp. 192-226). Cambridge: Cambridge University Press.
- Larson, C. U. (1992). *Persuasion: Reception and responsibility* (6th ed.). Belmont, CA: Wadsworth.
- LaTour, M. S., & Rotfeld, H. J. (1997). There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself. *Journal of Advertising, 26*(3), 45-59.
- LaTour, M. S., & Snipes, R. L. (1996). Don't be afraid to use fear appeals: An experimental study. *Journal of Advertising Research, 36*(2), 59-67.
- Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. New York: Springer.
- Leathers, D. G. (1992). *Successful nonverbal communications: Principles and applications*. New York: Macmillan.
- Lee, D. M. (1986). Usage pattern and sources of assistance for personal computer users. *MIS Quarterly, 10*(4), 313-325.
- Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 5). New York: Academic.
- Leventhal, H. (1971). Fear appeals and persuasion: The differentiation of a motivational construct. *American Journal of Public Health, 61*, 1208-1224.
- Levine, B. A., Moss, K. C., Ramsey, P. H., & Fleishman, R. (1978). Patient compliance with advice as a function of communicator expertise. *Journal of Social Psychology, 104*, 309-310.
- Lindsey, L. (2004). The influence of persuasive messages on attitude and subjective norm: A test of the theory of reasoned action. *Dissertation Abstracts International Section A: Humanities & Social Sciences, 64*(8-A), 2705.

- Lirtzman, S. I., & Shuv-Ami, A. (1986). Credibility of source of communication on products' safety hazards. *Psychological Reports, 58*, 707-718.
- 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.
- Luftman, J., & McLean, E. R. (2004). Key issues for it executives. *MIS Quarterly Executive, 3*(2), 89-104.
- Ma, Q., & Liu, L. (2005). The role of internet self-efficacy in the acceptance of web-based electronic medical records. *Journal of Organizational & End User Computing, 17*(1), 38-57.
- Maddux, J. E., & Rogers, R. W. (1980). Effects of source expertness, physical attractiveness, and supporting arguments on persuasion: A case of brains over beauty. *Journal of Personality and Social Psychology, 39*, 235-244.
- 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.
- Marakas, G. M., Yi, M. Y., & Johnson, R. D. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research, 9*(2), 126-163.
- McCroskey, J. C., & Jenson, T. J. (1975). Image of mass media news sources. *Journal of Broadcasting, 19*, 169-180.
- McGuire, W. J. (1968). Personality and susceptibility to social influence. In E. Borgatta & W. Lambert (Eds.), *Handbook of personality theory and research* (pp. 1130-1187). Chicago: Rand McNally.
- McGuire, W. J. (1969). The nature of attitudes and attitude change. In G. Lindzey & E. Aronson (Eds.), *The handbook of social psychology* (Vol. 3, pp. 136-314). Reading, MA: Addison-Wesley.
- McGuire, W. J. (1978). An information-processing model of advertising effectiveness. In H. L. Davis & A. J. Silk (Eds.), *Behavioral and management sciences in marketing* (pp. 156-180). New York, NY: Wiley.
- McKay, D. L., Berkowitz, J. M., Blumberg, J. B., & Goldberg, J. P. (2004). Communicating cardiovascular disease risk due to elevated homocysteine levels: Using the EPPM to develop print materials. *Health Education and Behavior, 31*(3), 355-371.

- Melone, N. P. (1990). A theoretical assessment of the user satisfaction construct in information systems research. *Management Science*, 36(1), 76-91.
- Mewborn, C. R., & Rogers, R. W. (1979). Effects of threatening and reassuring components of fear appeals on physiological and verbal measures of emotion and attitudes. *Journal of Experimental Social Psychology*, 15, 242-253.
- Miller, G., & Baseheart, J. (1969). Source trustworthiness, opinionated statements, and response to persuasive communication. *Speech Monographs*, 36, 1-7.
- Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, 2(3), 192-222.
- Mugny, G., Tafani, E., Falomir, P., Juan, M., & Layat, C. (2000). Source credibility, social comparison, and social influence. *Revue Internationale de Psychologie Sociale*, 13, 151-175.
- Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.
- O'Keefe, D. J. (1990). *Persuasion: Theory and research*. Newbury Park, CA: Sage.
- Ortony, A., & Turner, T. J. (1990). What's basic about basic emotions? *Psychological Review*, 97(3), 315-331.
- Pornpitakpan, C. (2004). The persuasiveness of source credibility: A critical review of five decade's evidence. *Journal of Applied Social Psychology*, 34(2), 243-281.
- Powell, F. (1965). Source credibility and behavioral compliance as determinants of attitude change. *Journal of Personality and Social Psychology*, 2, 669-676.
- Powell, F. C., & Wanzelried, J. W. (1995). Do current measures of dimensions of source credibility produce stable outcomes in replicated tests? *Perceptual and Motor Skills*, 81(2), 675-687.
- Rapoza, J. (2005). Spyware fracas heats up. *eWeek*, 22(11), 56.
- Rasmussen, M. (2004). *Demand for endpoint security growing*. Retrieved January 31, 2006, from <http://www.csoonline.com/analyst/report2170.html>
- Riemenschneider, C. K., Harrison, D. A., & Mykytyn, P. P. (2003). Understanding it adoption decisions in small business: Integrating current theories. *Information and Management*, 40(4), 269-285.

- Robey, D. (1979). User attitudes and management information systems use. *Academy of Management*, 22(3), 527-538.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, 93-114.
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protected motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153-176). New York, NY: The Guilford Press.
- Roskos-Ewoldsen, D. R., Yu, H. J., & Rhodes, N. (2004). Fear appeal messages affect accessibility of attitudes toward the threat and adaptive behaviors. *Communication Monographs*, 71(1), 49-69.
- Ross, J. A. (1973). Influence of expert and peer upon negro mothers of low socioeconomic status. *Journal of Social Psychology*, 89, 79-84.
- Schneider, T. R., Salovey, P., Pallonen, U., Mundorf, N., Smith, N. F., & Steward, W. T. (2001). Visual and auditory message framing effects on tobacco smoking. *Journal of Applied Social Psychology*, 31(4), 667-682.
- Schulman, G., & Worrall, C. (1970). Salience patterns, source credibility, and the sleeper effect. *Public Opinion Quarterly*, 34, 371-382.
- Schultz, R. L., & Slevin, D. P. (1975). Implementation and organizational validity: An empirical investigation. In R. L. Schultz & D. P. Slevin (Eds.), *Implementing operations research/management science* (pp. 153-182). New York, NY: American Elsevier.
- Segars, A. H. (1997). Assessing the unidimensionality of measurement: A paradigm and illustration within the context of information systems research. *OMEGA*, 25(1), 107-121.
- Shang, R. A., Chen, Y. C., & Shen, L. (2005). Extrinsic versus intrinsic motivation for consumer to shop on-line. *Information and Management*, 42(3), 401-413.
- Shaw, M. E., & Wright, J. M. (1967). Scales for the measurement of attitudes. New York: McGraw Hill.
- Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research*, 15(3), 325-343.

- Sherer, M., & Rogers, R. W. (1984). The role of vivid information in fear appeals and attitude change. *Journal of Research in Personality, 18*(3), 321-334.
- Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8*(1), 31-41.
- Stanley, M. A., & Maddux, J. E. (1986). Cognitive processes in health enhancement: Investigations of a combined protection motivation and self-efficacy model. *Basic and Applied Social Psychology, 7*(2), 101-113.
- Stephenson, M. T. (1993). *A subliminal manipulation of the extended parallel process model*. Texas A&M University.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.
- Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of AIS, 13*, 380-427.
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.
- Sutton, S. R. (1982). Fear-arousing communications: A critical examination of theory and research. In J. R. Eiser (Ed.), *Social psychology and behavioral medicine* (pp. 303-337). London: Wiley.
- Suzuki, K. (1978). Acceptance and rejection of a suggestion. *Japanese Psychological Research, 20*, 60-70.
- Swanson, E. B. (1982). Measuring user attitudes in MIS research: A review. *OMEGA International Journal of Management Science, 10*, 157-165.
- Swanson, E. B. (1988). *Information systems implementation: Bridging the gap between design and implementation*. Homewood, IL: Irwin.
- Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly, 15*(1), 125-143.
- Torkzadeh, G., & Dwyer, D. J. (1994). A path analytic study of determinants of information system usage. *OMEGA International Journal of Management Science, 22*(4), 339-348.
- Trandis, H. C. (1977). *Interpersonal behavior*. Monterey, CA: Brooke/Cole.

- Trow, M. (1993). *Managerialism and the academic profession: The case of England*. Berkeley, CA: The University of California at Berkeley.
- Tybout, A. M. (1978). Relative effectiveness of three behavioral influence strategies as supplements to persuasion in a marketing context. *Journal of Marketing Research*, 15, 229-242.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.
- 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.
- Venkatesh, V., & Speier, C. (1999). Computer technology training in the workplace: A longitudinal investigation of the effect of mood. *Organizational Behavior and Human Decision Processes*, 79(1), 1-28.
- Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the check-off password system (COPS): An advancement in user authentication methods and information security. *Journal of Organizational & End User Computing*, 16(3), 41-58.
- Warren, I. D. (1969). The effect of credibility in sources of testimony on audience attitudes toward speaker and message. *Speech Monographs*, 36, 456-458.
- Watts, W., & McGuire, W. J. (1964). Persistence of induced opinion change and retention of the inducing message contents. *Journal of Abnormal and Social Psychology*, 68, 233-241.
- Whaley, C. (2005, 1/14/2005). Security companies might be messing with it managers' minds. *Computing Canada*, 31, 17.
- Whitman, M. E. (2003). Enemy at the gate: Threat to information security. *Communications of the ACM*, 46(8), 91-95.
- Wildstrom, S. H. (2005, March 17, 2005). Ousting spyware from your PC. *Business Week Online*, 68-76.
- Wittaker, J. O., & Meade, R. D. (1968). Retention of opinion change as a function of differential source credibility. *International Journal of Psychology*, 3, 103-108.
- Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, 59, 329-349.

- Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs*, *61*, 113-134.
- Witte, K. (1998). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In P. A. Andersen & L. K. Guerrero (Eds.), *Handbook of communication and emotion: Research, theory, applications, and contexts* (pp. 423-450). San Diego, CA: Academic Press.
- 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*, 317-341.
- Witte, K., & Morrison, K. (1995). The use of scare tactics in aids prevention: The case of juvenile detention and high school youth. *Journal of Applied Communication Research*, *23*, 128-142.
- Wu, Y., Stanton, B. F., Li, X., Galbraith, J., & Cole, M. L. (2005). Protection motivation theory and adolescent drug trafficking: Relationship between health motivation and longitudinal risk involvement. *Journal of Pediatric Psychology*, *30*(2), 127-137.
- Yang, H. D., & Yoo, Y. (2004). It's all about attitude: Revisiting the technology acceptance model. *Decision Support Systems*, *38*, 19-31.

APPENDIX A
EXEMPLAR FEAR APPEALS

McAfee Hoaxes

Virus Hoaxes: Not Just Harmless Pranks

There are a lot of viruses out there. And then there are some viruses that aren't really out there at all. Hoax virus warning messages are more than mere annoyances. After repeatedly becoming alarmed, only to learn that there was no real virus, computer users may get into the habit of ignoring all virus warning messages, leaving them especially vulnerable to the next real, and truly destructive, virus.

Fortunately, AVERT tracks virus hoaxes as well as genuine viruses. The next time you receive an urgent virus warning message, check it against the list of known virus hoaxes below. If it's a hoax, chances are you'll find it in our database. And if it's a real virus, we'll probably know about it already, and you'll find it in the McAfee Virus Information Library.

Don't let your guard down!

Remember: Never open an email attachment unless you know what it is--even if it comes from someone you know and trust.

Be aware that the people who create viruses can use known hoaxes to their advantage. A good example is the AOL4FREE hoax. This began as a hoax warning about a nonexistent virus. Once it was known that this was a hoax, somebody began to distribute a destructive trojan horse (a trojan horse differs from a virus in that it does not reproduce itself) in a file named AOL4FREE, attached to the original hoax virus warning! The lessons are clear:

- Always remain vigilant
- Never open a suspicious attachment

Network Associates AntiSpyware

Network Associates Introduces McAfee AntiSpyware - Essential Protection Against Spyware for Consumers

Posted on 12 February 2004 | Other McAfee releases at HNS

Spyware, Web Dialers and Adware Now Account for Over Half of the Top 20 Malicious Threats Reported to McAfee Security

SANTA CLARA, Calif., Feb. 12 /PRNewswire-FirstCall/ -- Network Associates, Inc. (NYSE: NET), the leading provider of intrusion prevention solutions, today announced the immediate availability of McAfee AntiSpyware (MAS). McAfee AntiSpyware proactively detects and eliminates spyware, adware and potentially dangerous applications such as key loggers, behavior-tracking programs and browser hijackers before they are able to rob identities, steal passwords, modify or destroy files and monitor unsuspecting users' Internet activity. According to a study by the National Cyber-Security Alliance, 91 percent of all home PCs are infected with some kind of spyware today. These annoyances can advance to serious threats, such as fraud or even identity theft. McAfee(R) AntiSpyware helps keep vulnerable private information secure.

McAfee AntiSpyware addresses a clear and present market need for a more robust consumer spyware defense -- one that includes proactive, automated scanning for early detection of spyware, pre-emptive alerts to notify the user and block the program from executing on its own, as well as an easy-to-use interface. The first product to provide users with both on-demand scanning and proactive on-execution scanning, MAS automatically detects threats as they attempt to compromise a user's system. With MAS, home users can now take advantage of proactive protection around the clock.

"Viruses, while posing a significant threat, aren't the only dangers lurking on the Internet. Spying and tracking programs employ a number of deceptive techniques to remotely invade the PC -- often unbeknownst to the user," said Lisa Henderson, vice president of marketing with the McAfee Security Consumer division at Network Associates.

"Network Associates McAfee AntiSpyware provides advanced protection for the PC and personal data, has an early warning detection system, proactively protects users and their identities from suspicious programs and helps to ensure online privacy."

McAfee AntiSpyware includes the following components:

- Advanced "Auto-Protect" Technology alerts users when potentially hostile applications attempt to install and run, providing options to block the threat at the gateway.
- Multiple Scanning Options (On-Demand and On-Execution) allow users to perform thorough or custom scans depending on their need. The default setting performs a full system scan.
- One year of Automatic Updates prompt users to download and install the most up-to-date protection against spying and tracking programs.

- Extensive Detection Database provides a thorough database of adware, spyware and keylogging programs. This database is continuously updated to keep up with the plethora of programs created daily by hackers.
- Uninstall Flexibility allows you the choice to uninstall tracking programs using that program's uninstaller (if available), or McAfee AntiSpyware's removal technique, which removes all traces of the program.
- "One-Stop-Shop" Identification and Removal of all components and files associated with spyware; allowing users to remove any and all infected files in one click.

Users of P2P software may be particularly at risk of having spyware on their systems, as lack of attention to license agreements may result in the installation of unintended programs. By default, McAfee AntiSpyware quarantines all detected spyware and adware programs. Because users may want to retain some of these programs, they are given the option to "trust" the program so that it will not be detected in future scans. In addition, McAfee AntiSpyware provides easy restoration of programs that users may have inadvertently removed during previous scans.

Spyware is often used to track online behavior to more effectively target pop-up ads. The files associated with tracking behavior sit hidden on the hard drive, potentially slowing down the performance of the computer. Similarly, key-logging programs can be installed on a machine to secretly monitor everything that is typed. This monitoring may include Websites visited, personal passwords, chat room conversations and email. McAfee AntiSpyware detects keyloggers before they have a chance to record keystrokes and removes the spyware programs and files that otherwise may take over the hard drive. With McAfee AntiSpyware's enhanced protection that extends beyond anti-virus and firewall, users' data and identity are more secure than ever. McAfee AntiSpyware is an integral part of a layered PC protection strategy.

Webroot's Spyware Sweeper

PC Magazine's Best of the Year 2004 for antispyware, Spy Sweeper now scans for spyware 30% faster. Spy Sweeper detects and successfully removes vicious programs like CoolWebSearch. For advanced protection, Active Shields defend your browser and operating system from attempted spyware installations. Enhanced Internet Explorer shields block changes to your browser settings. Several operating system shields reinforce its ability to catch spyware when it attempts to download, install or run on a user's PC. Spy Sweeper subscribers receive effective anti-spyware coupled with the industry's most extensive research efforts. Its highly honed detection process uses a constantly updated definitions database to identify and safely quarantine the most cunning spyware. A dedicated threat research lab identifies new threats or existing threat variations, and pushes out new definitions as frequently as necessary. Subscribers report new spyware to the threat research team with an easy-to-use notification feature. A refined detection and quarantine process successfully roots out even the most devious spyware variants, like CoolWebSearch. Once spyware is detected, the quarantine feature allows users to safely manage spyware by removing, without harming other programs on the computer. Expert customer support, available via phone and email, help subscribers navigate any spyware-related issues. The Spy Sweeper user interface is simple and intuitive. Users pick what programs, files and folders to scan, and schedule automatic sweeps at a desired time, or choose to sweep on demand. Traditional anti-virus programs and firewalls don't offer protection from harmful spyware programs. The consequences of unidentified spyware can include identity theft and computer corruption. Spyware infections can occur when you visit a questionable web site, open spam, or download a free software program. Your privacy is at high risk if you surf the Internet, share your PC, or use file-sharing programs.

Microsoft AntiSpyware

Microsoft Windows AntiSpyware (Beta): Overview

Published: January 6, 2005

Microsoft Windows AntiSpyware (Beta) is a security technology that helps protect Windows users from spyware and other potentially unwanted software. Known spyware on your PC can be detected and removed. This helps reduce negative effects caused by spyware, including slow PC performance, annoying pop-up ads, unwanted changes to Internet settings, and unauthorized use of your private information. Continuous protection improves Internet browsing safety by guarding more than 50 ways spyware can enter your PC. Participants in the worldwide SpyNet™ community play a key role in determining which suspicious programs are classified as spyware. Microsoft researchers quickly develop methods to counteract these threats, and updates are automatically downloaded to your PC so you stay up to date.

Benefits

Detect and remove spyware	Improve Internet browsing safety	Stop the latest threats
<ul style="list-style-type: none"> • Easily detect spyware on your PC. Quickly and easily find spyware that can slow down your computer, display annoying pop-up ads, change Internet settings, or use your private information without your consent. 	<ul style="list-style-type: none"> • Help stop spyware in its tracks with continuous protection. Windows AntiSpyware improves Internet browsing safety by guarding more than 50 ways Web sites and programs can put spyware on your PC. 	<ul style="list-style-type: none"> • Stop new threats faster with SpyNet™. The voluntary, worldwide SpyNet™ community plays a key role in determining which suspicious programs are classified as spyware. SpyNet™ participants help to discover new threats quickly so everyone is better protected. Any user can choose to join SpyNet™ and report potential spyware to Microsoft.
<ul style="list-style-type: none"> • In-depth spyware removal returns your PC to normal. Straightforward operation and thorough removal technology make it easy for people of all skill levels to eliminate detected spyware. If you inadvertently remove any programs, you can easily get them back. 	<ul style="list-style-type: none"> • Protection that doesn't distract you from using your PC. Windows AntiSpyware works in the background, automatically handling spyware based on your preferences. This enables you to use your PC with minimal interruption. 	<ul style="list-style-type: none"> • Spyware expertise you can rely on. A dedicated team of Microsoft researchers scours the Internet to discover new spyware and develop methods to counteract it.
<ul style="list-style-type: none"> • Maintain your PC with regularly scheduled spyware scanning and removal. Regularly scheduled spyware scans help maintain your PC. 		<ul style="list-style-type: none"> • Automatically stay up to date. Updates to counteract new spyware are automatically downloaded to your PC.

Detect and remove spyware	Improve Internet browsing safety	Stop the latest threats
	<ul style="list-style-type: none"><li data-bbox="690 325 1031 577">• Undo unwanted changes to Internet Explorer settings. Easily restore Internet settings that are persistently changed by spyware, including your home page or the default search engine.	

APPENDIX B
SURVEY INSTRUMENT

Survey Instrument

Introduction

In today's highly inter-connected computing paradigm, people are at risk to any number of potential hazards to their data. Spyware represents a general form of threat by which software is installed on a person's computer with or without the knowledge of the operator. Some instances of spyware are essentially harmless, but annoying advertisement software. Other spyware infections pose a much more significant threat to data integrity and personal identity by capturing transmitted data or keystrokes.

Purpose

In order for us to improve the quality and availability of anti-spyware support provided to faculty, staff, and students at MSU, we seek your input. Please consider your personal concerns regarding spyware and spyware protection. Spyware protection refers to the use of anti-spyware for prevention, detection, and/or recovery from spyware.

The data obtained from this study will only be used in aggregate with no identification provided for individual responses. Participation in this survey is strictly voluntary and appreciated; however, there are no consequences for non-participation.

Section 1: General Purpose

Think about your usage and maintenance responsibilities for a specific computer system. Please select a single score from 1 to 5 where, 1 – means you **Strongly Disagree** with the statement, and 5 – means you **Strongly Agree** with the statement.

		Strongly Disagree (1)		Neutral (3)		Strongly Agree (5)
1.	I maintain important data on a specific computer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	I am responsible for the detection, prevention and/or removal of spyware from that computer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	I am concerned for the security of the data on that computer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Section 2: Spyware Threat Concerns

The following statements concern spyware and spyware protection. Anti-spyware use refers to installing, running, updating, and/or configuring the software. Please select a single score from 1 to 5 where, 1 – means you **Strongly Disagree** with the statement, and 5 – means you **Strongly Agree** with the statement.

		Strongly Disagree (1)		Neutral (3)		Strongly Agree (5)
1.	If my computer were infected by spyware, it would be severe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	If my computer were infected by spyware, it would be serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	If my computer were infected by spyware, it would be significant	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.	My computer is at risk for becoming infected with spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	It is likely that my computer will become infected with spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.	It is possible that my computer will become infected with spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.	Anti-spyware software is easy to use	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	Anti-spyware software is convenient to use	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.	I am able to use anti-spyware software without much effort	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.	Anti-spyware software works for protection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.	Anti-spyware software is effective for protection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.	When using anti-spyware software, a computer is more likely to be protected	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13.	I would find the use of anti-spyware software useful in my job	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14.	Using anti-spyware software enables me to accomplish tasks more quickly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15.	Using anti-spyware software increases my productivity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16.	If I use anti-spyware software, I will increase my chances of getting a raise	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		Strongly Disagree (1)		Neutral (3)		Strongly Agree (5)
17.	Using anti-spyware software would improve my job performance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18.	Using anti-spyware software will make it easier to do my job	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19.	People who are important to me think that I should use anti-spyware software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20.	People who influence my behavior think that I should use anti-spyware software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21.	The senior management of this University has been helpful in support of anti-spyware software use	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22.	In general, the University has supported using anti-spyware software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23.	I intend to use anti-spyware software in the next 3 months	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
24.	I predict I will use anti-spyware software in the next 3 months	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
25.	I plan to use anti-spyware software in the next 3 months	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
26.	Using the anti-spyware software is a good idea	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27.	Anti-spyware software makes work more interesting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
28.	Working with anti-spyware software is fun	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
29.	I like working with anti-spyware software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
30.	Working with anti-spyware software is enjoyable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Section 3: Message Feedback

Please indicate with a check mark in the appropriate box the term that best captures your beliefs concerning the *competence* of Mr. Craig Martin:

		Neutral							
31.	Experienced	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Inexperienced
32.	Expert	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Ignorant
33.	Trained	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Untrained
34.	Competent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Incompetent

Please indicate with a check mark in the appropriate box the term that best captures your beliefs concerning the *trustworthiness* of Mr. Craig Martin:

		Neutral							
35.	Just	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unjust
36.	Kind	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cruel
37.	Admiral	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Contemptible
38.	Honest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Dishonest
39.	Fair	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unfair

Please indicate with a check mark in the appropriate box the term that best captures your beliefs concerning the *dynamism* of Mr. Craig Martin:

		Neutral							
40.	Aggressive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Meek
41.	Bold	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Timid
42.	Energetic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tired
43.	Extroverted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Introverted

Section 4: Demographic Information

The demographic information in this section will only be used in aggregate form and will not be used to identify individual respondents. Please select only one item in each category. Experience refers to your experience using anti-spyware software. Department refers to the department in which you are employed or are enrolled as a student.

Gender	<input type="checkbox"/> male <input type="checkbox"/> female	Experience	<input type="checkbox"/> < 6 months <input type="checkbox"/> 6-12 months <input type="checkbox"/> > 1 year to 2 years <input type="checkbox"/> > 2 years to 3 years <input type="checkbox"/> > 3 years	Age	<input type="checkbox"/> 18 to 29 <input type="checkbox"/> 30 to 39 <input type="checkbox"/> 40 to 49 <input type="checkbox"/> 50 to 59 <input type="checkbox"/> 60 and over
Education	<input type="checkbox"/> high school <input type="checkbox"/> some college <input type="checkbox"/> bachelor's degree <input type="checkbox"/> master's degree <input type="checkbox"/> doctorate <input type="checkbox"/> other	Department	<input type="checkbox"/> COBI <input type="checkbox"/> CVM <input type="checkbox"/> ITS <input type="checkbox"/> CE <input type="checkbox"/> other		

Thank you for participating in this study.

APPENDIX C
FEAR APPEAL TREATMENT

From the ITS Offices of MSU
Principle Contact: Craig Martin
Re: Spyware

Date: July 1, 2005

Currently, 91% of all home PCs are infected with some kind of spyware. Spyware is a form of software that can install itself on computer systems with or without the consent of the computer's operator. Even anti-virus software, such as Norton Anti-virus, is useless in stopping a spyware attack. The effects of spyware may be disastrous, as some form of it may lead to fraud or identity theft.

Anti-spyware software provides a proven method for protecting against spyware. This software works automatically to detect and remove existing installations of spyware and to proactively guard against future intrusions. The software is easy to install and most come with an intuitive interface that provides a clear and consistent method for fine tuning the performance of the software to match the desires of the user.

It is recommended that all faculty, staff, and students of Mississippi State University take the appropriate steps to obtain and install anti-spyware software. Freeware copies of the software are available on the University's ITS web site.

Respondent Instructions

Thank you for participating in this study. As you know, no attempts to identify individual responses will be made at any time in this research.

In this experiment you will be exposed to a message that contains arguments advocating the installation and use of anti-spyware software. The first message will be a typed document, the other a video of Mr. Craig Martin. Mr. Martin is an experienced Information Technology professional and has been active in numerous positions of influence for the advancement of secure computing for the University as well as the state of Mississippi.

If, for any reason, you are not able to view the streaming video of Mr. Martin, please indicate as such when asked on a follow-up question.