MIS Quarterly

SPECIAL ISSUE

FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY[1]

By: **Allen C. Johnston**
Department of Management, Information Systems, and Quantitative Methods
School of Business
University of Alabama at Birmingham
1530 Third Avenue South
Birmingham, AL 35294-4460
U.S.A.
ajohnston@uab.edu

Merrill Warkentin
Department of Management and Information Systems
College of Business
Mississippi State University
P.O. Box 9581
Mississippi State, MS 39762-9581
U.S.A.
mwarkentin@acm.org

Abstract

Information technology executives strive to align the actions of end users with the desired security posture of management and of the firm through persuasive communication. In many cases, some 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 investigate the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions toward the mitigation of threats. An examination was performed that culminated in the development and testing of a conceptual model representing an infusion of technology adoption and fear appeal theories.

Results of the study suggest that fear appeals do impact end user behavioral intentions to comply with recommended individual acts of security, but the impact is not uniform across all end users. It is determined in part by perceptions of self-efficacy, response efficacy, threat severity, and social influence. The findings of this research contribute to information systems security 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 mitigation.

Keywords: Information security, countermeasures, protection motivation theory, fear appeals, persuasive communication, information assurance, threat appraisal, coping appraisal

Introduction

Within the modern business climate, organizations commonly suffer from threats to corporate data, information technology infrastructure, and personal computing. According to the 2007 Computer Crime and Security Survey, conducted jointly by the Computer Security Institute and the San Francisco Office of the Federal Bureau of Investigation, 46 percent of respondents reported some form of security incident during the past year (Richardson 2007). Moreover, security incidents, such as viruses, system penetrations, insider abuse, or

[1]M. Adam Mahmood was the accepting senior editor for this paper.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

other forms of unauthorized access continue to increase in sophistication and impact, with the average annual loss reported by U.S. companies doubling from $168,000 in 2006 to $350,424 in 2007 (Richardson 2007). Interestingly, these figures may understate the magnitude of the information security problem facing organizations in that we know historically that most organizations seek to maintain a low profile and refuse to comment on their information assurance practices and security breaches (Hoffer and Straub 1989).

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 threats (Straub and Welke 1998). IT professionals strive to instill a consistent approach to assurance through policies and procedures that govern end user computing (Straub and Welke 1998; Siponen 2000). Security management is an especially challenging area in that end users vary widely in their level of threat awareness and knowledge of how to control their respective computing facilities (Siponen 2000). Also, the large differential among end users in terms of access privileges, priority, and motivation further complicates compliance efforts (Siponen 2000).

End users operating in decentralized environments in which they share or maintain sole responsibility for their computing resources commonly receive input from others regarding the most effective information assurance practices (Warkentin and Johnston 2006, 2008). The intention of such guidance is to steer end user actions toward behaviors that are consistent with the assurance goals of management or of the firm (Warkentin and Johnston 2008). For high-level managers desiring reliable responses from their end user community, the use of persuasive communications may be especially appealing (Goodhue and Straub 1991).

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 embedded in various artifacts to which end users are exposed (O'Keefe 1990; Rogers 1983). For example, persuasive messages can be incorporated into interdepartmental communications or IT security training and awareness materials. Persuasive messages may also be embedded into applications as popup dialog boxes, which, in turn, can be triggered by logical or temporal circumstances.

The present study investigates the effectiveness of persuasive messages in motivating end users to take action to secure their own computing environment. The persuasive messages of interest are those that include the element of threat, known as fear appeals, which have been the subject of numerous studies across a wide variety of domains (Hoog et al. 2005). In order to facilitate this research, we examine a specific type of threat—spyware—which is an increasingly notorious and noxious form of malware found in nearly all computing settings (Arnett and Schmidt 2005). Spyware is illicit code that has been surreptitiously placed on a host computer by a foreign agent (Warkentin, Luo, and Templeton 2005). It has the potential to monitor and capture sensitive information from an unprotected computer system by sending that information over the Internet without the knowledge of the host (Schmidt and Arnett 2005).[2] Hence, the term spyware.

The purpose of this study is to examine the influence of fear appeals on behavioral intentions, specifically the compliance of end users. It focuses on recommendations to enact specific individual computer security actions that are believed to mitigate threats. Study findings should be generalizable to the impact of fear appeals in all decentralized environments in which end users exercise some degree of autonomous control over IT resources. The purpose of a fear appeal is to effect change through persuasion (Roskos-Ewoldsen et al. 2004), which is not required within centralized IT governance environments characterized by mandatory IT actions (Warkentin and Johnston 2006, 2008). Thus, the primary research question to be addressed in this study is: *How do fear appeals modify end user behavioral intentions associated with recommended individual computer security actions?* This question will be pursued by employing an empirical research design based on the theoretical foundations of protection motivation theory (PMT) augmented with behavioral antecedents typically associated with technology adoption scenarios.

The remainder of this paper will proceed as follows. First, the conceptual and theoretical background relating to PMT will be presented. Then our research model is presented, along with hypotheses for the present study. The next section will discuss the methodology in detail, and this is followed by project findings. Finally, implications are discussed, along with project limitations and opportunities for future research.

Conceptual Background

Simply put, a fear appeal is a persuasive message with the intent to motivate individuals to comply with a recommended

[2]Spyware can also adversely affect the productivity of end users by slowing down their systems.

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.

Threat

As defined by Witte (1992), a threat is an external stimulus that exists whether or not it is perceived by an individual. If an individual perceives the threat, that individual can be described as having awareness of a threat. A properly constructed fear appeal not only serves to induce cognitions that a threat exists but also serves to convey the severity of the threat and its target population's susceptibility to the threat (Rogers 1975; Witte 1992). From this message, an individual is able to formulate *perceived threat severity* and *perceived threat susceptibility* (Rogers 1975; Witte 1992; Witte et al. 1996). 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 probability of personally experiencing the threat.

Efficacy

A fear appeal will contain arguments that cause an individual to form cognitions about efficacy. This perception of efficacy includes: (1) cognitions of the efficacy of the recommended response and (2) 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. 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.

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 the fear appeal research 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. A pioneering theory of fear and motivation, the fear-as-acquired drive model was 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 and McGuire, have since been overwhelmingly rejected (Beck and 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 and Rogers 1979).

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). 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 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.

Building on Leventhal's parallel process model, Rogers' (1975) protection motivation theory 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. His later work (Rogers 1983) resulted in the addition of a fourth component, self-efficacy, to PMT. It was Rogers' contention that when all of these components are at moderate-to-high

levels, an individual's protection motivation would also be at a moderate-to-high level, thereby increasing the probability of change in his or her attitude and behavioral intent.

According to Witte (1992), a fear appeal has 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 (1) providing unambiguous and feasible steps to avert the threat and (2) highlighting the value of the recommended response in averting the threat. PMT 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.

In circumstances where a fear appeal is successful in eliciting a significant perception of threat, an evaluation of the efficacy of the response (response efficacy) and one's ability to enact the response (self-efficacy) immediate follows. In situations in which perceived threat is accompanied by a moderate-to-high degree of perceived efficacy, individuals will take action to mitigate 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. The danger control process is one that can lead to positive outcomes; this is the user response that IT managers wish to promote when they utilize fear appeals in the security context. Accordingly, the focus of this research project is to measure indicators of the danger control process—the desired outcome—that may result from the fear appeal.

PMT is an established, robust theoretical foundation for the analysis and exploration of recommended actions or behaviors to avert the consequences of threats. PMT has experienced broad empirical support, primarily in the application of fear appeals directed toward threats and actions such as the use of condoms to prevent the spread of HIV. The recommended actions associated with fear appeals typically incorporate nontechnological solutions such as breast self-exams or smoking cessation. However, in the application domain of the present study, namely IT-based solutions to computer security threats, a clear technology adoption component is present in the individual user's decision to comply with the recommended action.

PMT forms the basis of the conceptual model (FAM) to be tested in this study and provides the theoretical support for an individual's cognitive appraisals of threat and efficacy when confronted with a fear appeal. A fear appeal includes a recommended response to a threat, and as is so often the case in the information security context, the response is technology use oriented. In this study, the recommended response was the use of anti-spyware software. As such, we were compelled to consult the technology adoption literature and extend PMT to include technology adoption components, namely *social influence* and *behavioral intent*.[3] Social influence plays an important role in determining how users will react to technology use (Venkatesh and Davis 2000; Venkatesh et al. 2003), especially when persuaded to do so via a social cue (fear appeal). Fear appeals are a mechanism through which social influence is imposed. Given the nature of this study concerns persuasive communication, influences from family, friends, colleagues, or trusted others within the organization are highly important and must be accounted for.

Conceptual Model and Hypotheses Development

Based on causal and outcome variables espoused in fear appeal theory and augmented with antecedents of technology-dependent behavioral intent, we propose a fear appeals model (FAM). The model explains user intentions to engage in individual computer security actions recommended in fear-inducing persuasive communications. As shown in Figure 1, the model is an extension of the danger control process as described by PMT. Social influence is included in the model as a direct determinant of behavioral intent and aids in predicting intentions to accept and use a particular security technology.

As illustrated in Figure 1, perceptions of threat severity and susceptibility are positioned as direct antecedents of response efficacy and self-efficacy and indirectly influence behavioral intent. Behavioral intent is directly influenced by perceptions of response efficacy, self-efficacy, and social influence.

To test FAM, we needed to study a threat that affects many end users and about which there was some general awareness. Further, the threat proxy for this study needed be one in which

[3] A previous version of FAM included the *performance expectancy* construct from Venkatesh et al.'s (2003) unified theory of acceptance and use of technology (UTAUT). The construct was removed during pilot testing due to its nonsignificant impact on the dependent variable, behavioral intent.

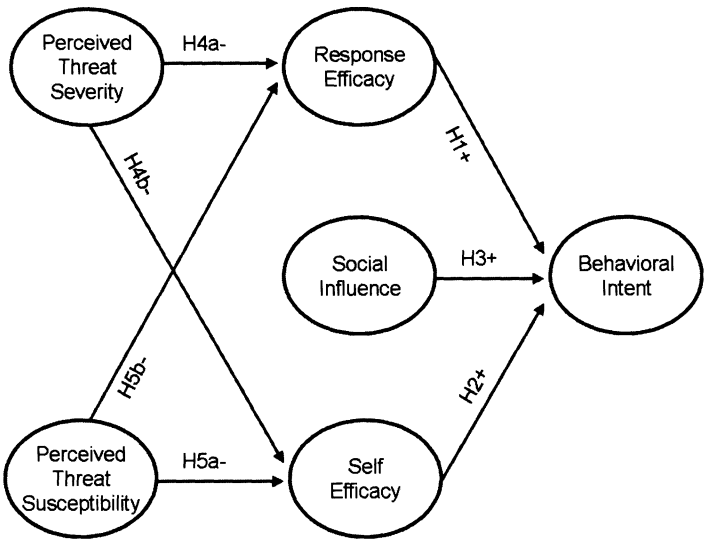

Figure 1. Fear Appeals Model (FAM)

autonomous users within a decentralized IT environment would be able to take actions to mitigate. Considerable press has been given to the dangers and methods for mitigation of spyware. Spyware is a particularly devious form of malicious code that can invade a computer and compromise not only the functionality of the resource but also the privacy of the user. Additionally, these infections can occur with the consent of the operator or without consent, in which case the software can perform undetectable surveillance and reporting of the operator's computing activities.

Each year new and more sinister threats to end user information resources emerge; these are the threats that warrant persuasive communications (fear appeals) to end users because organizations have yet to establish practices for successful defense, or because users are not yet diligent in their approach to protecting themselves. For this study, spyware serves as an appropriate proxy for that sort of threat. The purpose of a fear appeal is to elevate perceptions of threat and efficacy regardless of any preconceptions the fear appeal audience may have held concerning the threat prior to exposure to the fear appeal message. If the fear appeal is effective, perceptions of threat and efficacy will be increased to sufficient levels at which point the end users will follow the recommended response.

Direct Effects on Behavioral Intent

In the proposed model, we articulate the two dimensions of perceived efficacy, response efficacy and self-efficacy, as direct determinants of intent. Response efficacy refers to the degree to which an individual believes a recommended response will effectively avert a threat (Rogers 1975; Witte 1992). 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 (Rogers 1983). According to PMT, moderate to high levels of response efficacy are associated with positive inclinations of threat mitigation 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 anti-spyware solution and form a disposition toward the recommendation based on this appraisal. It is with this background that the following hypothesis is offered:

H_1: Response efficacy will have a positive effect on end user intentions to adopt recommended individual computer security actions with respect to spyware.

High levels of emotional arousal are thought to have a negative impact on self-efficacy (Kavanagh and Bower 1985; Lazarus and Folkman 1984; Marakas et al. 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, result in lower levels of perceived capability to

use a computer. The rationale is that as threatening events, such as viral attacks, Trojan activities, spyware infestations, or rootkit infestations, are perceived as more severe or probable, end users may start to doubt their ability to function adequately within the heightened threat conditions without causing harm to data or their computing environment. Further, Gutek and Winter (1990) argue that high levels of emotional arousal are associated with degraded end user performance.

Similar to the manner in which an individual cognitively assesses the efficacy of a response, he or she also appraises the ability to carry out the recommendation (Maddux and Rogers 1983; Witte 1992). First established by Maddux and Rogers (1983) and Rogers (1983) as an extension of PMT, self-efficacy is regarded as a determinant of intent 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 will still consider his or her ability to successfully install and run the anti-spyware solution. From this argument, we offer the following hypothesis:

H_2: Self-efficacy will have a positive effect on end user intentions to adopt recommended individual computer security actions with respect to spyware.

A 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 colleagues and others whose opinions matter support its acceptance and use (Hartwick and Barki 1994; Venkatesh et al. 2003). This determinant is referred to as *social influence*, which has a long history and has most recently been placed in a larger context as part of technology adoption literature.

Social influence closely resembles *social norm*, which was determined to be a significant direct determinant of behavioral intent in the theory of reasoned action (Fishbein and Ajzen 1975) and the theory of planned behavior (Ajzen 1991; Venkatesh and Davis, 2000). In those theories, it was determined that a person's intentions to perform a behavior is 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, Higgins, and Howell's (1991) construct *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.

We argue that computer users will engage in explicit discussions as well as implicit activities concerning the appropriate actions to take toward the security of their communications. Venkatesh and Davis (2000) suggest that the rationale for the direct effect of social influence on behavioral intent is that

> people may choose to perform a behavior, even if they are not themselves favorable toward the behavior or its consequences, if they believe one or more important referents think they should, and they are sufficiently motivated to comply with the referents (p. 187).

The referents of interest in this study may be a peer group or, at the very least, the communicating IT official. 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. As this guidance is provided within an organizational setting, it typically originates from persons in positions of authority and emphasizes compliance with perceived norms within the firm. Further, Lewis et al. (2003) state that, "if a peer, supervisor, or some other actor in a relevant social network believes that a technology is useful, through a process of shared cognition, so will the target individual" (p. 662). It is with this understanding that we offer the following hypothesis:

H_3: Social influence will have a positive effect on end user intentions to adopt recommended individual computer security actions with respect to spyware.

Threat Effects

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 that a fear appeal's audience holds toward the significance of the threat (Rogers 1975; Witte 1992). PMT defines perceptions of threat severity to be the ability to influence the intensity of a response. It does so by directly manipulating perceptions of both response efficacy and self-efficacy. For example, as an end user's perception of the severity of a spyware threat increases, beliefs regarding the capabilities of anti-spyware software to adequately address the threat decline (Witte 1992). Additionally, variations in the perceived severity of the spyware threat cause end users to reassess their

ability to successfully enact anti-spyware protection. As the threat is perceived to be more severe, an end user will feel less able to effectively address the threat. From this argument, the following hypotheses are offered:

H_{4a}: *Perceptions of threat severity will negatively influence perceptions of response efficacy.*

H_{4b}: *Perceptions of threat severity will negatively influence perceptions of self-efficacy.*

Perceived 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 influences the downstream relationships between an end user's intent 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 influence (Rogers 1975; Witte 1992).

In a study of fear appeals in the context of AIDS prevention, Witte (1994) determined that as individuals were provided literature highlighting the prevalence and pervasiveness of the AIDS epidemic, the participants' perceptions of their ability to protect themselves from the danger and of the efficacy of condom use were weakened. A similar study concerning the threat of contracting a sexually transmitted disease produced the same results; as perceptions of threat susceptibility increased, perceptions of efficacy (response and self) decreased (Witte et al. 1996). In the context of spyware defense, it is expected that perceptions regarding a particular anti-spyware solution to effectively and efficiently provide protection will decrease in strength as the threat of such an attack becomes more probable. As such, the following hypotheses are offered:

H_{5a}: *Perceptions of threat susceptibility will negatively influence perceptions of response efficacy.*

H_{5b}: *Perceptions of threat susceptibility will negatively influence perceptions of self-efficacy.*

Methodology

An experiment was selected as the appropriate methodology to study the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions toward the mitigation of threats. Although conducted as a laboratory experiment with university subjects, this is an appropriate group for the objectives of the study (Gordon et al. 1986). Faculty, staff, and student groups are frequently susceptible to the threat of spyware. Moreover, their responses to fear appeals and to assessments of their capabilities, other perceptions, and behavioral intent to use anti-spyware software are valuable metrics for testing FAM as a whole. Whereas we would not argue that this sample is highly generalizable to the overall citizenry, it is reasonable that it could be generalized to university settings and to educated professional and administrative workers, perhaps even to professional and administrative knowledge workers in industry and nonprofit organizations.

Measures and Instrumentation

Six constructs were measured in this study: behavioral intent (BINT), social influence (SINF), response efficacy (RESP), self-efficacy (SEFF), threat severity (TSEV), and threat susceptibility (TSUS). The constructs were multi-item scales drawn from previously validated measures and were adapted to relate specifically to the context of security responses to spyware. BINT and SINF were adapted from Venkatesh et al. (2003), while RESP, SEFF, TSEV, and TSUS were adapted from Witte et al. (1996). All items were assessed via a five-point Likert scale. One of the constructs, social influence, was determined to be comprised of causal indicators and subsequently regarded as a formative construct. A formative construct is composed of indicators that may have little correlation with each other, as they represent unique dimensions of the construct (Jarvis et al. 2003). The implications of this distinction are many and include the manner in which the scales used to measure the constructs are validated and the method by which the structural model is tested.

Content validity for all instrument scales (both formative and reflective) was established through both literature review and a content validity expert panel comprised of eight faculty and doctoral students skilled in quantitative analysis and quantitative research methods. Particularly for formative constructs, content validity is critical, as removal of items from formative scales must be theoretically driven and must not compromise scale robustness by removing items that capture critical dimensions of the latent variables (Diamantopoulos and Winklhofer 2001; Straub et al. 2004). The results of the content validity panel review were that two items pertaining to social influence would be dropped. The rationale for their removal was that they were viewed as redundant and contributing to an unnecessarily lengthy instrument without capturing a unique dimension within the construct.

Experimental Design and Procedure

Approximately 780 faculty, staff, and students from multiple units at one large university were solicited via e-mail to volunteer for the project. The university's information security management strategy was highly decentralized, thereby placing a large burden on the end user population to actively participate in information security procedures. Anti-malware solutions, such as anti-spyware software, were made available to end users, but their use was not mandated, monitored, nor automated on behalf of the users. Further, we sought a broad sample of experienced computer users with a degree of autonomous control over their computer and its data, and who held sensitive data worth protecting. As such, the first three items of the survey instrument were used to ensure some degree of autonomy over security actions (see Appendix A). No incentives were offered. A total of 311 subjects participated (40 percent response rate), with 275 producing usable data. Approximately 61 percent were male with 63 percent being from the college of business. A majority (73 percent) were between the ages of 18 and 29, reflecting the sampling frame, largely drawn from computer-savvy student groups.

As described by Leventhal (1970), the typical experimental design for studies concerning the impact of fear appeals on behavioral intent is the classical design. In the classical design, the study participants are split into two groups. One group of participants is exposed to some form of communication and surveyed as to the impact of the stimulus prior to and after the treatment, while a second group, the control group, is merely surveyed without exposure to the treatment. By adding a third group, a modified classical design is created. The third group is exposed to the communication, but is surveyed only after the treatment exposure and not before. This modified design provides an additional level of assurance that any change in perceptions is the result of the treatment as opposed to sources of internal bias such as history, maturation effect, or testing (Babbie 2004; Campbell and Stanley 1963; Cook and Campbell 1979).

Based on this modified classical design, willing participants were randomly assigned to three groups such that group 1 had, at a minimum, an N of 200, group 2 had an N of 30, and group 3 had an N of 30. Group 1 participants were exposed to a pretest survey followed by a fear appeal treatment and a posttest survey, while group 2 participants were subjected only to the pretest survey and the posttest survey—thus, the classic experimental design. The pretest and posttest surveys are identical (Appendix A), thereby ensuring accurate measurement. As mentioned previously, a third group (group 3), subjected to the fear appeal treatment and the posttest survey only, makes it possible to account for testing effects, thereby providing some assurance of internal validity (Shadish et al. 2001). While tests of fear appeal manipulation and internal validity require only a sample size of 30 from each group, group 1 (pretest–treatment–posttest) was assigned a much larger N so as to provide an adequate sample space for subsequent tests of the FAM nomology. Ultimately, the sample size for group 1 was 215.

Experimental Treatment

Traditional applications of fear appeals are found in the areas of healthcare and marketing (LaTour and Rotfeld 1997; LaTour and 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 mitigate the threat, thereby avoiding the negative consequences. Furthermore, these types of fear-inducing persuasive messages have been proven to be successful in inciting changes in attitude, behavioral intent, and behavior (Schneider et al. 2001; Sherer and Rogers 1984).

As described earlier, a fear appeal is comprised of two important elements: (1) statements alluding to both the severity and susceptibility dimensions of a threat and (2) statements pertaining to both the efficacy of the audience and of the response in alleviating the threat (Witte 1992). In this case, the threat was presented as the invasive software referred to as spyware. Therefore, statements to encourage and support the abilities of the respondents as well as the capability of the anti-spyware software were included in the fear appeal. Because the participants of the study operated in an environment in which they maintained autonomy over their respective computing facilities and because an enterprise-wide solution or policy for spyware protection was not yet established or enforced, a fear appeal concerning anti-spyware use was both relevant and timely.

One might expect that, prior to the experiment, the study participants would have already formed impressions concerning the threat of spyware (threat susceptibility and threat severity) as well as the efficacy of the recommended anti-

spyware response (response efficacy) and their ability to perform the recommended response (self-efficacy). Any group of users will have a wide range of perspectives regarding any specific threat. Fear appeals may reinforce the beliefs of some users and may elevate the beliefs of others. In either case, the users will act if sufficiently motivated. The purpose of the fear appeal is to elevate perceptions of threat and efficacy in order to elicit a reaction consistent with the desires of management. Any previously held perceptions of efficacy or threat would only serve as a baseline from which the users' perceptions might change depending on their reaction to the fear appeal. The purpose of this research was to investigate this reaction.

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, 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.

A fear appeal message review panel comprised of marketing experts verified the validity of the fear appeal treatment. This expert group was knowledgeable about the fear appeal literature and was also experienced in performing content validity tests; it consisted of eight faculty and doctoral students. They gauged the ability of the treatment to convey certain information considered necessary in a fear appeal and, upon completion of their review, they made suggestions for clarity and improvement in conveying threat and efficacy which were implemented.

Data Analysis and Results

The following sections detail the data analysis procedures involved in this study. Included in this discussion are descriptions of instrument validity tests, a manipulation check, an internal validity test, and an assessment of FAM. Following the description of the analyses, the results are described and presented in model and tabular format.

Instrument Validity

Because social influence is a formative construct, a component-based technique for structural equation modeling, such as partial least squares (PLS), is required. Group 1 (N = 215) posttest response data were used for these validity tests. For tests of convergent and discriminant validity of the formative independent variable, one possible validation approach is to examine patterns of correlation between items and constructs (Petter et al. 2007). Diamantopoulos and Winklhofer (2001) propose that formative items should correlate with a "global item that summarizes the essence of the construct" (p. 272). PLS item weights, which indicate the impact of individual formative items (Bollen and Lennox 1991), can be multiplied by item values and summed, as noted by Bagozzi and Fornell (1982). In effect, this results in a modified multitrait, multimethod (MTMM) matrix of item-to-construct and item-to-item correlations similar to that analyzed by Bagozzi and Fornell as well as Loch et al. (2003). The resulting matrix, showing item-to-construct correlations as grayed out cells, appears as Table 1.[4]

Following the logic of Campbell and Fiske (1959), Loch et al. (2003) suggest that convergent validity is demonstrated if items of the same construct correlate significantly with their corresponding composite construct value (item-to-construct correlation). This condition has been met, as all items correlated significantly ($p < 0.01$) with their respective construct composite value. The results, therefore, indicate an acceptable level of convergent validity.[5]

Discriminant validity can be established if item-to-construct correlations are higher with each other than with other construct measures and their composite values (Loch et al. 2003). This condition is also met.

Construct validity tests were also conducted for the reflective variables. Factor 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 load (Straub et al. 2004). Generally, convergent validity is demonstrated if (1) the item loadings are in excess of 0.70 on their respective factors and (2) average variance extracted (AVE) for each construct is above 0.50 (Gefen and Straub 2005). As indicted in Table 2, these con-

[4]Also included in this analysis for the purpose of comparison are the formative variables "Performance Expectancy" and "Attitude" toward anti-spyware use (Shaw and Wright 1967).

[5]Another test of convergent validity examines the PLS item weights for significance (Petter et al. 2007). These weights were found to be significant.

Table 1. Inter-Item and Item-to-Construct Correlation Matrix

	PERF1	PERF2	PERF3	PERF	SINF1	SINF2	SINF	ATTI1	ATTI2	ATTI3	ATTI4	ATTI
PERF1	–											
PERF2	0.618	–										
PERF3	0.536	0.747	–									
PERF	0.909	0.880	0.768	–								
SINF1	0.376	0.381	0.419	0.436	–							
SINF2	0.312	0.294	0.289	0.344	0.340	–						
SINF	0.413	0.403	0.419	0.466	0.759	0.870	–					
ATTI1	0.224	0.312	0.364	0.313	0.300	0.085	0.216	–				
ATTI2	0.255	0.317	0.341	0.329	0.331	0.127	0.261	0.776	–			
ATTI3	0.251	0.315	0.344	0.326	0.353	0.117	0.266	0.689	0.806	–		
ATTI4	0.241	0.296	0.369	0.316	0.315	0.063	0.208	0.725	0.848	0.836	–	
ATTI	0.274	0.343	0.392	0.358	0.361	0.117	0.270	0.862	0.938	0.916	0.936	–

PERF = Performance Expectancy; SINF = Social Influence; ATTI = Attitude

Table 2. Loadings, Cross-Loadings, and AVEs for Multi-Item Constructs

	TSEV	TSUS	SEFF	RESP	BINT	AVE
TSEV1	.922	.101	.050	.121	–.025	
TSEV2	.915	.182	.034	.140	.084	.846
TSEV3	.820	.264	.059	.166	.127	
TSUS1	.268	.846	–.022	.082	.066	
TSUS2	.058	.926	.087	.003	–.014	.780
TSUS3	.197	.820	.140	.001	.104	
SEFF1	.054	.096	.894	.067	.168	
SEFF2	.056	.065	.904	.209	.096	.846
SEFF3	.027	.050	.895	.022	.176	
RESP1	.122	.022	–.007	.887	.085	
RESP2	.168	–.004	.169	.875	.153	.792
RESP3	.120	.066	.140	.819	.212	
BINT1	.093	.083	.156	.214	.886	
BINT2	.013	.063	.159	.193	.914	.873
BINT3	.067	.018	.144	.063	.912	

TSEV = Threat Severity; TSUS = Threat Susceptibility; SEFF = Self-Efficacy; RESP = Response Efficacy; BINT = Behavioral Intent; AVE = Average Variance Extracted

Table 3. Reliability and Inter-Construct Correlations

		Inter-Construct Correlations				
Construct	CRel	TSEV	TSUS	SEFF	RESP	BINT
TSEV	0.943	**0.920**				
TSUS	0.914	0.673	**0.883**			
SEFF	0.942	0.143	0.183	**0.919**		
RESP	0.897	0.322	0.114	0.304	**0.864**	
BINT	0.954	0.344	0.155	0.342	0.369	**0.934**

Shaded items are square root of average variance extracted (AVE); CRel = Composite Reliability

Table 4. Manipulation Check Results

IV	F-test	Significance
TSEV	6.850	$p < 0.01$
TSUS	6.174	$p < 0.05$
SEFF	8.988	$p < 0.01$
RESP	10.344	$p < 0.01$

TSEV = Threat Severity; TSUS = Threat Susceptibility; SEFF = Self-Efficacy; RESP = Response Efficacy

ditions have been met. Gefen and Straub (2005) also contend that discriminant validity is demonstrated if (1) the square root of each construct's AVE is greater than the interconstruct correlations and (2) item loadings on their respective constructs are greater than their loadings on other constructs. As indicated in Table 2, these conditions have also been met, thereby demonstrating that the independent construct indicators discriminate well.

Finally, reliability for the scales was gauged via composite reliability scores provided in the PLS output. Composite reliability scores equal to or greater than 0.70 are regarded as acceptable (Fornell and Larker 1981; Gefen and Straub 2005). As indicated in Table 3, the composite reliability scores of these reflective variables are acceptable.

Manipulation Check

In an effort to ensure that the subjects of the experiment were successfully manipulated by the fear appeal treatment, they were given a general question as to whether or not they completely read the fear appeal. A discriminant analysis of the variables TSEV, TSUS, SEFF, and RESP, using subject (all groups; N = 275) responses to the general question as a grouping variable was conducted. The findings of this analysis, reported in Table 4, suggest that differentials in the variables TSEV, TSUS, SEFF, and RESP were caused by the application of the fear appeal treatment and that the subjects were, consequently, aware of the manipulation.

Fear Appeal Manipulation and Test of Internal Validity

To assess whether the fear appeal treatment was effective in manipulating perceptions of TSEV, TSUS, SEFF, and RESP, a within-subjects MANCOVA of group 1 (N = 215) (pretest–treatment–posttest) response data was conducted. Two individual characteristics, age and experience with anti-spyware software, were included in the analysis as covariates. The results of this analysis provide an indication as to the effectiveness of the fear appeal (Appendix B) in eliciting a change in end user perceptions of RESP, SEFF, TSEV, and TSUS. These findings are reported in Appendix C and indicate that when exposed to the fear appeal treatment, previously reported perceptions of TSEV, TSUS, SEFF, and RESP increased significantly.[6] Given that these four variables are all addressed within the language of the fear appeal treatment, the significant differences in perceptions following

[6]ANCOVA results indicate no significant main effects of the covariates age and experience with anti-spyware software.

exposure to the appeal is not surprising and confirms that the fear appeal treatment was effective.

Finally, the differentials in the independent variables based on a MANOVA involving group 1 (pretest–treatment–posttest) and group 3 (treatment–posttest) were not significant ($p > 0.10$) for any of the independent variables, meaning that there were no significant differences between two groups of subjects (neither of which were exposed to the fear appeal treatment) in the mean value of TSEV, TSUS, SEFF, and RESP. These results suggest that the pretest condition was not a significant factor and the internal validity of the experimental design was sufficient. These results are also reported in Appendix C.

PLS Analysis: Test of FAM Nomology

A PLS analysis involving posttest group 1 data ($N = 215$) was used to test the structural model and its associated hypotheses. Through the use of a bootstrapping resampling procedure, the analysis produced estimates of both the path coefficients as well as the explained variance in RESP, SEFF, and BINT. Of the seven hypotheses, all but the two involving the influence of TSEV were found to be significant, as shown in the overall findings in Table 5. Explained variance for the FAM model was also reasonable. Overall, we conclude that the FAM model has received good support.

As indicated in Table 5 and Figure 2, the model explains approximately about 27 percent, 11 percent, and 4 percent of the variance. The highest explanatory power of 27 percent is the path for social influence, response efficacy, and self-efficacy leading to behavioral intent. Consistent with H_1, response efficacy has a significant positive effect on behavioral intent ($\beta = .213$, $p < .01$). Similarly, H_2 and H_3 are supported as both self-efficacy ($\beta = .187$, $p < .01$) and social influence ($\beta = .298$, $p < .001$) have significant positive effects on behavioral intent.

The results of the structural model analysis also confirm the negative relationships between perceptions of threat severity and threat susceptibility on response efficacy and self-efficacy. Combined, the two threat variables are able to explain approximately 4 percent of the variance in self-efficacy and 11 percent of the variance in response efficacy. H_{4a} and H_{4b} are supported as threat severity has a significant effect on both perceptions of response efficacy ($\beta = -.286$, $p < .01$) and self-efficacy ($\beta = -.437$, $p < .001$). The results indicate that the relationships between threat susceptibility and response efficacy ($\beta = -.079$, $p > .10$) as well as that of threat susceptibility and self-efficacy ($\beta = -.112$, $p > .10$) are not significant, thereby rendering H_{5a} and H_{5b} unsupported.

Discussion and Contribution

The results of the structural model testing indicate strong support for a model (FAM) that contextualizes the PMT danger control process in the technology adoption literature. With the exception of H_5, all other hypotheses were supported, indicating FAM has good explanatory power and a strong message for both scholars and practitioners. The downstream affect of the fear appeal treatment is evident not only in the significance of the paths linking response efficacy, self-efficacy, and social influence with behavioral intent, but also in the significant relationship between threat severity and the two dimensions of perceived efficacy (both response efficacy and self-efficacy). In an effort to maintain a parsimonious model which extends PMT, we limited the inclusion of further constructs that may have increased its explanatory power, and thus we explained a relatively small degree of variance in response efficacy and self-efficacy.

Interestingly, while both response efficacy and self-efficacy appear to have strong predictive ability, social influence has slightly more of an effect on behavioral intent. While elements of social influence were no doubt apparent in the fear appeal treatment, PMT does not position it as a core component of a fear appeal. As such, content validity tests of the fear appeal treatment, conducted in an effort to form moderate to high levels of intensity in the language addressing perceived threat and efficacy, were not sensitive to how intensive social influence might be. Therefore, the research design did not directly control for social influence, allowing for heightened levels of perceived intensity. Furthermore, because students undoubtedly experience significant influence to adopt security protocols, including the use of anti-spyware software, it is evident that such social influence was widely experienced before the present study's treatment. This factor contributes to the heightened level of influence of social influence on behavioral intent.

Finally, lack of support for H_5 (both H_{5a} and H_{5b}), while not consistent with PMT, is consistent with the findings of numerous other studies in which individualistic personas are exposed as confident in the face of threats to the greater population of end users. Previous studies concerning the perceptions of threat susceptibility by individual users found that, in general, individuals perceive themselves to be less likely to experience a malicious attack than their peers (Loch

Table 5. Overview of Findings

Hypothesis (with Direction)	Path Coefficient (β)	F or T Value	P-Value	Supported?
H_1: RESP → BINT (+)	0.213	2.52	p < 0.01	Supported
H_2: SEFF → BINT (+)	0.187	2.43	p < 0.01	Supported
H_3: SINF → BINT (+)	0.298	4.55	p < 0.001	Supported
H_{4a}: TSEV → RESP (-)	–0.286	3.16	p < 0.01	Supported
H_{4b}: TSEV → SEFF (-)	–0.437	5.61	p < 0.001	Supported
H_{5a}: TSUS → RESP (-)	–0.079	0.77	p > 0.10	Not supported
H_{5b}: TSUS → SEFF (-)	–0.112	1.73	p > 0.10	Not supported

RESP = Response Efficacy; SEFF = Self-Efficacy; SINF = Social Influence; TSEV = Threat Severity; TSUS = Threat Susceptibility; and BINT = Behavioral Intent

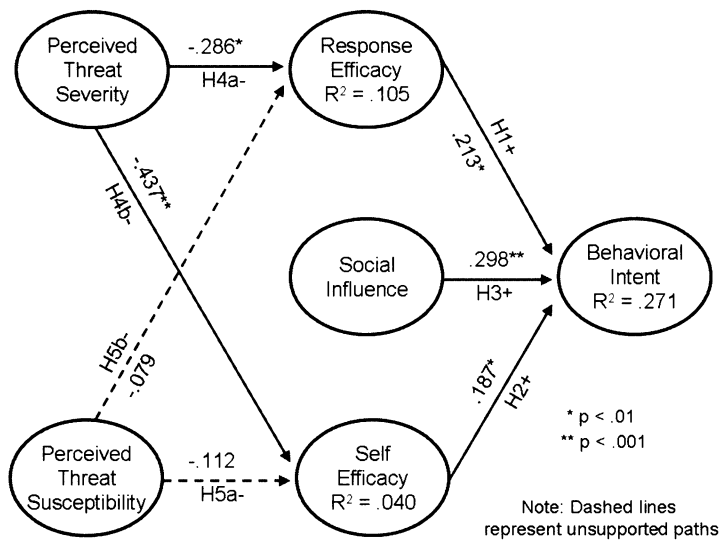

Figure 2. Results of FAM PLS Structural Model Analysis

et al. 1992; Schmidt and Arnett 2005). Loch et al. (1992) offer that individuals often see threats as affecting others more than themselves, thus "exhibiting a rather naïve belief that bad things only happen to other people" (p. 185). Croog and Richards (1977) suggest that previous negative experiences with similar threats or knowledge or others with previous detrimental experiences can influence the perception one has toward the probability of malicious outcomes. Without such cues, it is likely that a sense of invincibility may persist. As such, fear appeals should reinforce the probability of occurrence with concrete examples of the negative outcomes directly related to a threat.

This study contributes to the field of information systems by applying a well-established theory for explaining human reaction to fear-inducing messages from the domain of social psychology to the domain of IS studies. PMT represents a culmination of years of research and improvements to fear appeal theory, and its impact within the realm of IS research, particularly information security, is promising.

While technology adoption theories (e.g., TAM/UTAUT) offer powerful models for predicting user behavior within the domain of information technology acceptance, they have been limited in their ability to explain the acceptance and use of

security technology because they do not include the concept of threat and are most often geared toward productivity-based applications. While productivity-based software tools such as spreadsheets and word processors can improve job performance, many security technologies impede performance (Warkentin et al. 2004; Warkentin et al. 2007) in an effort to secure the working environment. As our study shows, the perception of threat is an essential component of the motivation to use protective software. The security domain clearly calls for the additional insights into threat and efficacy as suggested by PMT and FAM.

Chief security officers and other IT security managers face the challenge of encouraging and motivating end user constituents to observe information security policies and to implement security-related procedures (Warkentin and Johnston 2008). While numerous researchers have pointed to the use of emotional messages to inspire end users to practice safe computing, no study has conceptualized and tested a model for predicting how users will respond to fear-inducing communications. This study provides a contribution in this respect and provides IT managers with insight for tailoring their fear appeals for maximum effectiveness. Specifically, if managerial communications appeal to users' perceptions of threat severity and susceptibility as well as users' self-efficacy and perception of response efficacy, then the desired result should be enhanced. That is, our research indicates that properly worded communications will spur responses from users that are consistent with the organization's goals with regard to the adoption of secure behaviors.

Whereas the present study's experiment focused on anti-spyware use, individuals motivated to act securely in one phase of the security action cycle (Straub and Welke 1998) would similarly be motivated to engage in other safe behaviors. Accordingly, the results of this study support the use of fear-inducing arguments as an effective way to influence end user intentions to carry out recommended individual security actions. However, the findings indicate that these messages inspire different outcomes for different users based on their perceptions of efficacy and threat. Consistent with Figure 1, individuals will react to fear-inducing arguments in one of two ways: message rejection or message acceptance (Witte 1992). Messages warning of new threats and advising a plan of action to counter the threat will inspire some users to accept the message and take appropriate action to reduce the threat. For others, their reaction may be to reject the message and to take action to reduce their fear (Witte 1992), thereby leaving some vulnerabilities unaddressed and exposing the entire firm to potential harm. Therefore, a singular 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.

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 our results suggest, end users are not consistent in their behavioral intentions 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, may exhibit a significant increased vulnerability profile (Warkentin and Willison, 2009). Accordingly, security managers may wish to reevaluate their IT security governance strategy to ensure the greatest level of user compliance with organizational security policy.

Limitations and Future Research

McGrath (1982) describes the "three horned dilemma" to highlight the trade-offs between various research designs, and argues that all empirical designs are subject to inherent limitations. Various research designs may result in greater or less (1) generalizability to the target population, (2) precision in measurement and control of the behavioral variables, and (3) realism of context. Probably the two most significant limitations of our experimental design derive from an attempt to test a parsimonious model within a reasonable time frame and with a realistically sized instrument. For this reason, constructs such as propensity to trust and propensity to fear were not considered and should be included in future studies.

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 respondent schedules prohibited a longitudinal research design in this case. 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. In another setting, though, this is a viable extension of the current work.

One possible limitation of this research is found in the fact that most of the subjects were between the ages of 18 and 29. In a recent article, however, Knight and Pearson (2005)

detected no differences among the various age ranges regarding computer behavior in the workplace. Considering that behavior is determined by behavioral intentions, the exact ramifications of a limited age spectrum on the generalizability of the findings remains unclear.

Another possible limitation is its use of faculty, staff, and students as subjects. Our findings can be generalized to university settings and other environments in which decentralized IT governance structures are employed and in which users exercise some degree of autonomy. Decentralized environments, including most universities, are generally less secure than those characterized by a centralized governance structure with rigorous standards, procedures, controls, and sanctions (Warkentin and Johnston 2008). As a result, the 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, and decisions to act to address relevant threats may not be regarded as a high priority among end users. Additionally, the "open" nature of a university may limit social norms from being articulated as frequently or as adamantly among peers or between management and end users as required for effective threat defense. Given the strong empirical support for the relationship between social influence and behavioral intent, this should be an area of concern for IT managers and a topic of interest for future research activities.

The decision to include students as part of the sample space is supported by the findings of Dickson et al. (1986) and also by Niederman and DeSanctis (1995), who found that a pool consisting of student subjects can be generalized to a larger population, especially when the phenomenon of interest is one in which the students are familiar. University students are exposed to and must react to malicious threats as well as fear appeal messages designed to modify their behaviors. Further, the widespread use of students as human subjects in IS research published in leading business journals (e.g., Agarwal and Karahanna 2000; Gefen et al. 2003; Jarvenpaa and Leidner 1999; Warkentin et al. 2004; Warkentin et al. 1997) legitimizes the use of student data (Stablein 1999). While numerous previous studies concerning computer security and information assurance have involved higher education employees or students (Aytes and Connolly 2004; Warkentin et al. 2004), we fully acknowledge that this sample may limit generalizability. Research in the future should test the generalizability of our finding via different subject pools and organizational environments.

Finally, PMT forms the basis of the conceptual model (FAM) to be tested in this study, but because the recommended solution to a security threat is often technology use oriented, we also incorporated the technology adoption elements of social influence and behavioral intent. Based on a rigorous assessment of the constructs employed in previous technology adoption studies (TAM, TAM2, UTAUT), it was determined that social influence was the most applicable measure for this study of persuasive communications in the security context and would be incorporated into the FAM model. It is the vehicle by which social influence is conveyed. Other technology adoption elements such as perceived ease of use and usefulness are applicable only to productivity-enhancing technologies such as spreadsheets and word processors, for example. Further, TAM2 and UTAUT did not include attitude for reasons of parsimony. We followed this approach and did not include attitude in our conceptual model either.

In conclusion, the present work gives managers a set of practical courses of action. It also suggests ways that researchers can explore the domain of information security. Fear appeals and the other variables studied are thus an attractive means for securing the workplace and could productively occupy the IS community for some time to come.

References

Agarwal, R., and Karahanna, E. 2000. "Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology," *MIS Quarterly* (24:4), pp. 665-694.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Arnett, K. P., and Schmidt, M. B. 2005. "Busting the Ghost in the Machine," *Communications of the ACM* (48:8), pp. 92-95.

Aytes, K., and Connolly, T. 2004. "Computer Security and Risky Computing Practices: A Rational Choice Perspective," *Journal of Organizational & End User Computing* (16:3), pp. 22-40.

Babbie, E. 2004. *The Practice of Social Research*, Belmont, CA: Wadsworth/Thomson Learning.

Bagozzi, R. P., and Fornell, C. 1982. "Theoretical Concepts, Measurement, and Meaning," in *A Second Generation of Multivariate Analysis*, C. Fornell (ed.), New York: Praeger.

Beck, K. H., and Frankel, A. 1981. "A Conceptualization of Threat Communications and Protective Health Behavior," *Social Psychology Quarterly* (44:3), pp. 204-217.

Bollen, K. A., and Lennox, R. 1991. 'Conventional Wisdom on Measurement: A Structural Equation Perspective," *Psychological Bulletin* (110:2), pp. 305-314.

Campbell, D. T., and Fiske, D. W. 1959. "Convergent and Discriminant Validation by the Multi-Trait–Multi-Method Matrix," *Psychological Bulletin* (56:2), pp. 81-105.

Campbell, D. T., and Stanley, J. 1963. *Experimental and Quasi-Experimental Designs for Research*, Chicago, IL: Rand McNally.

Cook, T. D., and Campbell, D. T. 1979. *Quasi Experimentation: Design and Analytical Issues for Field Settings*, Chicago, IL: Rand McNally.

Croog, S. H., and Richards, N. P. 1977. "Health Beliefs and Smoking Patterns in Heart Patients and Their Wives: A Longitudinal Study," *American Journal of Public Health* (67:10), pp. 921-930.

Diamantopoulos, A., and Winklhofer, H. 2001. "Index Construction with Formative Indicators: An Alternative to Scale Development," *Journal of Marketing Research* (38:2), pp. 269-277.

Dickson, G. W., DeSanctis, G., and McBride, D. J. 1986. "Understanding the Effectiveness of Computer Graphics for Decision Support: A Cumulative Experimental Approach," *Communications of the ACM* (29:1), pp. 40-47.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior*, Reading, MA: Addison-Wesley.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equations with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), pp. 51-90.

Gefen, D., and Straub, D. W. 2005. "A Practical Guide to Factorial Validity using PLS-Graph: Tutorial and Annotated Example," *Communications of the AIS* (16:25), pp. 91-109.

Goodhue, D., and Straub, D. W. 1991. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures," *Information and Management* (20:1), pp. 13-27.

Gordon, M. E., Slade, L. A., and Schmitt, N. 1986. "The 'Science of the Sophomore' Revisited: From Conjecture to Empiricism," *Academy of Management Review* (11:1), pp. 191-207.

Gutek, B. A., and Winter, S. J. 1990. "Computer Use, Control Over Computers, and Job Satisfaction," in *People's Reactions to Technology, The Claremont Symposium on Applied Social Psychology,* S. Oskamp, and S. Spacapan, (eds.), Newbury Park, CA: Sage Publications.

Hartwick, J., and Barki, H. 1994. "Explaining the Role of User Participation in Information System Use," *Management Science* (40:4), pp. 440-465.

Hoffer, J. A., and Straub, D. W. 1989. "The 9 to 5 Underground: Are You Policing Computer Crimes?," *Sloan Management Review* (30:4), pp. 35-43.

Hoog, N. D., Stroebe, W., and Wit, J. B. 2005. "The Impact of Fear Appeals on Processing and Acceptance of Action Recommendations," *Personality and Social Psychology Bulletin* (31:1), pp. 24-33.

Hovland, C., Janis, I. L., and Kelly, H. 1953. *Communication and Persuasion*, New Haven, CT: Yale University Press.

Janis, I. L. 1967. "Effects of Fear Arousal on Attitude Change: Recent Developments in Theory and Experimental Research," in *Advances in Experimental Social Psychology*, L. Berkowitz (ed.), New York: Academic Press, pp. 166-225.

Jarvenpaa, S., and Leidner, D. 1999. "Communication and Trust in Global Virtual Teams," *Organization Science* (10:6), pp. 791-815.

Jarvis, C. B., Mackenzie, P. M., and Podsakoff, P. M. 2003. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journal of Consumer Research* (30:2), pp. 199-218.

Kavanagh, D. J., and Bower, G. H. 1985. "Mood and Self-Efficacy: Impact of Joy and Sadness on Perceived Capabilities," *Cognitive Theory and Research* (9), pp. 507-525.

Knight, M. B., and Pearson, J. M. 2005. "The Changing Demographics: The Diminishing Role of Age and Gender in Computer Usage," *Journal of Organizational & End User Computing* (17:4), pp. 49-65.

LaTour, M. S., and 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), pp. 45-59.

LaTour, M. S., and Snipes, R. L. 1996. "Don't be Afraid to Use Fear Appeals: An Experimental Study," *Journal of Advertising Research* (36:2), pp. 59-67.

Lazarus, R. S., and Folkman, S. 1984. *Stress, Appraisal, and Coping*, New York: Springer Publishing.

Leventhal, H. 1970. "Findings and Theory in the Study of Fear Communications," in *Advances in Experimental Social Psychology,* L. Berkowitz (ed.), New Yorik: Academic Press.

Leventhal, H. 1971. "Fear Appeals and Persuasion: The Differentiation of a Motivational Construct," *American Journal of Public Health* (61), pp. 1208-1224.

Lewis W., Agarwal, R., and Sambamurthy, V. 2003. "Sources of Influence on Beliefs about Information Technology Use: An Empirical Study of Knowledge Workers," *MIS Quarterly* (27:4), pp. 657-678.

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

Loch, K. D., Straub, D. W., and Kamel, S. Kamel. 2003. "Diffusing the Internet in the Arab World: The Role of Social Norms and Technological Culturation," *IEEE Transactions on Engineering Management* (50:1), pp. 45-63.

Maddux, J. E., and Rogers, R. W. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19), pp. 469-479.

Marakas, G. M., Yi, M. Y., and 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), pp. 126-163.

McGrath, J. 1982. "Dilemmatics: The Study of Research Choices and Dilemmas," in *Judgement Calls in Research*, J. McGrath, J. Martin, and R. Kulka (eds.), Beverly Hills, CA: Sage Publications, pp. 69-103.

McGuire W. J. 1968. "Personality and Susceptibility to Social Influence," in *Handbook of Personality Theory and Research*, E. Borgatta and W. Lambert (eds.), Chicago: Rand McNally, pp. 1130-1187.

McGuire W. J. 1969. "The Nature of Attitudes and Attitude Change," in *The Handbook of Social Psychology*, G. Lindzey and E. Aronson (eds.), Reading, MA: Addison-Wesley, pp. 136-314.

Mewborn, C. R., and 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* (15:3), pp. 242-253.

Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp. 192-222.

Niederman, F., and DeSanctis, G. 1995. "The Impact of a Structured-Argument Approach on Group Problem Formulation," *Decision Sciences* (26:4), pp. 451-474.

O'Keefe, D. J. 1990. *Persuasion: Theory and Research*, Newbury Park, CA: Sage Publications.

Petter S., Straub, D. W., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp. 623-656.

Richardson, R. 2007. "2007 CSI/FBI Computer Crime and Security Survey," Computer Security Institute (http://www.gocsi.com/press/20070913.jhtml).

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

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protected Motivation," in *Social Psychophysiology: A Sourcebook*, J. T. Cacioppo, and R. E. Petty (eds.), New York: The Guilford Press.

Roskos-Ewoldsen, D. R., Yu, H. J., and Rhodes, N. 2004. "Fear Appeal Messages Affect Accessibility of Attitudes Toward the Threat and Adaptive Behaviors," *Communication Monographs* (71:1), pp. 49-69.

Schmidt, M. B., and Arnett, K. P. 2005. "Spyware: A Little Knowledge is a Wonderful Thing," *Communications of the ACM* (48:8), pp. 67-70.

Schneider, T. R., Salovey, P., Pallonen, U., Mundorf, N, Smith, N. F., and Steward, W. T. 2001. "Visual and Auditory Message Framing Effects on Tobacco Smoking," *Journal of Applied Social Psychology* (31:4), pp. 667-682.

Shadish, W. R., Cook, T. D., and Campbell, D. T. 2001. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*, New York: Houghton-Mifflin Publishers.

Shaw, M. E., and Wright, J. M. 1967. *Scales for the Measurement of Attitudes*, New York: McGraw Hill.

Sherer, M., and Rogers, R. W. 1984. "The Role of Vivid Information in Fear Appeals and Attitude Change," *Journal of Research in Personality* (18:3), pp. 321-334.

Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management and Computer Security* (8:1), pp. 31-41.

Stablein. R. 1999. "Data in Organization Studies," in *Studying Organizations: Theory and Method*, S. Clegg and C. Hardy (eds.), London: Sage Publications, pp.255-271.

Straub, D. W., Boudreau, M. C., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of AIS* (13), pp. 380-427.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Sutton, S. R. 1982. "Fear-Arousing Communications: A Critical Examination of Theory and Research," in *Social Psychology and Behavioral Medicine*, J. R. Eiser (ed.), London: Wiley, pp. 303-337.

Thompson, R. L., Higgins, C. A., and Howell, J. M. 1991. "Personal Computing: Toward a Conceptual Model of Utilization," *MIS Quarterly* (15:1), pp. 125-143.

Venkatesh, V., and Davis, F. D. 2000. "A Theoretical Extension of the Technology Acceptance Model," *Management Science* (46:2), pp. 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.

Warkentin, M., Davis, K., and 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), pp. 41-58.

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

Warkentin, M., and Johnston, A. C. 2008. "IT Governance and Organizational Design for Security Management," in *Information Security: Policies, Processes, and Practices*, D. W. Straub, S. Goodman, and R. L. Baskerville (eds.), Armonk, NY: M. E. Sharpe, pp. 46-68.

Warkentin, M., Luo, X., and Templeton, G. F. 2005. "A Framework for Spyware Assessment," *Communications of the ACM* (48:8), pp. 79-84.

Warkentin, M., Sayeed, L., and Hightower, R. 1997. "Virtual Teams Versus Face-to-Face Teams: An Exploratory Study of a Web-Based Conference System," *Decision Sciences* (28:4), pp. 975-996.

Warkentin, M., Shropshire, J. and Johnston, A. C. 2007. "The IT Security Adoption Conundrum: An Initial Step Toward Validation of Applicable Measures," *Proceedings of the 2007 Americas Conference on Information Systems*, Keystone, CO, August 9-11.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs* (59), pp. 329-349.

Witte, K. 1994. "Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM)," *Communication Monographs* (61), pp. 113-134.

Witte, K., Cameron, K. A., McKeon, J. K., and Berkowitz, J. M. 1996. "Predicting Risk Behaviors: Development and Validation f a Diagnostic Scale," *Journal of Health Communication* (1), pp. 317-341.

About the Authors

Allen C. Johnston is an assistant professor in the School of Business at the University of Alabama Birmingham. He holds a BS from Louisiana State University in Electrical Engineering as well as an MSIS and a Ph.D. in Information Systems from Mississippi State University. His works can be found in such outlets as *Communications of the ACM*, *Journal of Global Information Management*, *DATA BASE for Advances in Information Systems*, *Journal of End User Computing*, *Journal of Information Privacy and Security*, *Journal of Internet Commerce*, and *International Journal of Information Security and Privacy*. The primary focus of his research has been in the areas of technology adoption, information assurance, and security, with a specific concentration on the behavioral aspects of information security and privacy.

Merrill Warkentin is Professor of MIS and FoB Notable Scholar at Mississippi State University. His research, primarily in information assurance and security, eCommerce, and virtual teams, has been published in books, proceedings, and journals such as *MIS Quarterly*, *Decision Sciences*, *European Journal of Information Systems, Decision Support Systems*, *DATA BASE for Advances in Information Systems*, *Communications of the ACM*, *Communications of the AIS*, *Information Systems Journal*, *Information Resources Management Journal*, *Journal of End User Computing*, and *Journal of Global Information Management*. Dr. Warkentin is the coauthor or editor of four books, and is serving or has served as associate editor or guest editor of *MIS Quarterly*, *European Journal of Information Systems*, *Information Resources Management Journal, Journal of Information Systems Security*, and others. Dr. Warkentin has served as a consultant to numerous organizations and has served as National Distinguished Lecturer for the Association for Computing Machinery (ACM).