PREVENTIVE ADOPTION OF INFORMATION SECURITY BEHAVIORS

Completed Research Paper

Donald Wynn, Jr.
University of Dayton
Dayton, OH 45469-2130 USA
dwynn1@udayton.edu

Clay K. Williams
Southern Illinois University
Edwardsville
Edwardsville, IL 62026 USA
cwillaa@siue.edu

Elena Karahanna
University of Georgia
Athens, GA 30602 USA
ekarah@uga.edu

Ramana Madupalli
Southern Illinois University
Edwardsville
Edwardsville, IL 62026 USA
rmadupa@siue.edu

Abstract

Many tools and safe computing practices are available to information system users to help them avoid the negative outcomes due to information security threats. Yet many users do not use these tools and practices. We seek to understand the factors influencing organizational users' adoption of preventive information security behaviors. These behaviors are similar to those which individuals practice to prevent negative health outcomes. A new model incorporating the primary antecedents of users' intentions related to preventive security, the Preventive Adoption Model (PAM), is presented and tested. PAM is derived from health behavior theories (health belief model, protection motivation theory, and theory of planned behavior) and integrates key constructs specific to the information security context. Results of the study suggest that users' beliefs regarding the threats and their avoidability, the proposed preventive actions, and their individual capabilities have an impact on their intentions to perform the prescribed behaviors.

Keywords: IS threat prevention, information security behaviors, security beliefs, Preventive Adoption Model, Health Belief Model, Prevention Motivation Theory

Introduction

> *"Various technologies are being brought to bear for security purposes, but if your end users are careless with their information or capabilities to get into applications, it will not matter whether you have state-of-the-art security technology in place" (Von Solms 2001).*

This quote highlights what many information security (infosec) experts have suggested for years: the weakest link in any security plan or procedure is the users themselves. It is the rare user that is completely aware of the latest in security risks and the often simple techniques for preventing them. Instead, many users simply do not engage in preventive computer security practices and behaviors. For example, many recent attempted attacks have been "spear phishing" seeking to exploit a known vulnerability in Microsoft's Internet Explorer 6 although newer versions of the software exist along with patches to close the vulnerability. This practice allowed a hacker to access Google's systems in late 2009. Other high-profile attacks include:

> In 2008, a Virginia investment firm accidentally exposed a number of private files to the outside world, including files containing the name and social security number of 2000 clients such as Supreme Court Justice Stephen Breyer.
>
> Also in 2008, computers at the campaign headquarters of presidential candidates Barack Obama and John McCain were hacked, apparently by a foreign attacker looking for policy documentation (Whitehouse et al. 2010).

These attacks exemplify the serious threats that are detrimental to the ability of individuals and organizations to secure and retain control of their information assets. Although there is no way to completely safeguard all of the information stored on an organization's information systems (IS), there are a number of ways that the volume of these attacks can be reduced. Recently, a group of United States Senators (Whitehouse et al. 2010) and a coalition of 28 commercial and governmental organizations (including Facebook, IBM, Microsoft, and the FBI) led an effort urging consumers to be mindful of ways to protect themselves, their employers, and the Internet community at large against cybercrimes.

Similar educational and promotional efforts aimed at reducing behavioral health risks such as tobacco usage, sedentary lifestyles, unhealthy diets, and alcohol usage have been relatively common for several decades (Glanz et al. 2008). The goal is to influence individuals to change their behaviors voluntarily in ways conducive to optimal health. These interventions are based on a number of health behavior theories which were developed to explain and influence the desired changes among a targeted set of individuals.

Similarities between preventive health behaviors and preventive security behaviors allow IS researchers to leverage similar behavioral theories to explain why many users do not engage in practices which would reduce or eliminate many of the risks associated with infosec threats such as viruses, spyware, and phishing. Recently, research articles have highlighted efforts to adapt these health behavior theories to the practice of preventive information security behaviors. These adaptations have been based on theories such as the Health Belief Model, the Protection Motivation Theory, and the Theory of Planned Behavior.

Adapting prominent models from the health behavior literature we develop a new model of preventive information security behaviors. This model utilizes concepts and relationships from health behavior theories to explain users' adoption of information security practices. The model is empirically tested using survey data collected from 256 users across organizations.

Health Behavior Theories

A preventive innovation is an adoption made at a given point in time to avoid or lower the probability of an event occurring in the future (Rogers 1995, p.70). Generally, these innovations have a slow rate of diffusion for several reasons. The necessity for the innovation is uncertain because we cannot say for sure that the negative event would have ever happened. If the preventive actions are in fact needed at some point, it may not happen until much later, which reduces any immediately perceived benefits. Further, the costs of prevention may be so high as to approach any possible losses or consequences. Individuals are often reluctant to adopt preventive innovations because of a combination of unpleasant, costly, or difficult behavioral changes along with an uncertain probability of any adverse circumstances occurring.

Two contexts in which such preventive innovations commonly exist are health care and information security. In both areas, individuals are susceptible to various intrusions or attacks, which may result in a wide range of potentially adverse circumstances. Many of these attacks can be thwarted by the internal systems and defensive mechanisms of the human body or the information system, respectively. However, these responsive measures are not always fully capable of defending every possible negative action. Many times, the most effective (if not the only) means of addressing these attacks involves specific behavioral practices or habits that either avoid the negative outcomes altogether or at least minimize their negative impacts. For health prevention, this includes such behaviors as regular medical checkups, dietary habits, immunizations, and the avoidance of risky behaviors (e.g. smoking, excessive drinking, driving without a seat belt, etc.). For information security specific behavioral practices include password management, email activities, and internet-surfing behaviors, the installation of defensive software tools, and automatic software updates for installed software applications and operating systems.

The health prevention and information security fields are both engaged in research efforts to increase the adoption of these preventive behaviors. Given the common goal of understanding and promoting "healthier" behaviors, we propose that research to understand the adoption of preventive information security behaviors can benefit from adopting theories explaining the adoption of preventive health behaviors. For this, we look to reference theories proposed in the preventive health behavior literature.

Health prevention research has focused on the behavioral issues associated with (among other things) ways to increase the adoption of measures intended to decrease the likelihood of occurrence of various illnesses and accidents. The most commonly applied preventive health behavior theories are the Health Belief Model (Rosenstock 1966; Rosenstock 1974), the Protection Motivation Theory (Rogers 1975; Rogers 1983), and the Theory of Planned Behavior (Ajzen 1991). Next we examine each of these theories en route to the development of a research model to investigate preventive information security behaviors.

The Health Belief Model (HBM) posits that an individual's likelihood to engage in preventive health behaviors such as health screenings, flu vaccinations, and dental checkups is a function of the perceived threat of the illness or condition to be avoided and the net benefit to the individual (Rosenstock 1974). Threat assessment is evaluated as the perceived severity and susceptibility of the condition to be avoided, whereas the benefits or efficacy of the preventive behaviors are evaluated net of perceived barriers to performing these behaviors (in terms of cost, effort, difficulty, access, etc.). It was also theorized that an additional stimulus or "cue to action" is required to trigger the actualization of the behavior.

Protection Motivation Theory (PMT) theorizes that a person's motivation to engage in self-protective behaviors is based on two cognitive processes: threat appraisal and coping appraisal (Prentice-Dunn and Rogers 1986; Rogers 1983). The threat appraisal process consists of assessing the severity and vulnerability of failing to engage in the self-protective behavior. Severity assesses the degree of harm that results from not engaging in the self-protective behavior, while vulnerability assesses the likelihood that such harm will occur. The process also involves assessing the rewards of engaging in maladaptive behaviors (e.g. the rewards of not giving up smoking). The rewards are offset by the perceived severity and vulnerability of any resulting threats. Threat appraisal is the sum of these factors. Coping appraisal is the sum of the individual's judgments regarding the effectiveness of the preventive behavior (response efficacy) and their ability to perform the behavior successfully (self-efficacy), minus any costs of doing so (such as inconvenience, expense, or difficulty). Threat appraisal and coping appraisal are combined to form an individual's protection motivation, which is most often measured as behavioral intention.

PMT is most often measured as six antecedents (severity, susceptibility, fear or threat, self-efficacy, response efficacy or effectiveness, and costs) directly associated with intention to perform a given protective behavior, whether avoiding a maladaptive response or initiating an adaptive response. A recent meta-analysis, found all six antecedents to be significantly associated with intentions (Milne et al. 2000).

Lastly, the Theory of Planned Behavior (TPB), while a general theoretical framework of behavior, has been used by researchers investigating the adoption of health behaviors, including smoking, contraceptive use, exercise behavior, and kidney donation. TPB extends the Theory of Reasoned Action (TRA) to include behaviors that are not completely under an individual's deliberate or volitional control. As with TRA, an individual's attitude toward a given behavior and the perceived subjective norms associated with the

behavior (including all relevant referents) influence the actual intentions to perform that behavior. Attitude is a function of the relevant beliefs about the behavior and its consequences. Likewise, subjective norm is a function of the beliefs that specific important to the individual parties think the individual should perform the behavior. Additionally, TPB incorporates perceived behavioral control which is the individual's "perceived ease or difficulty of performing the behavior" (Ajzen 1991). This construct is a function of the control beliefs a person has regarding their control over performing the behavior, including past experiences and anticipated obstacles, and it is a direct antecedent of behavioral intentions.

Application of Health Behavior Theories to Information Security

Information security research has leveraged the health behavior models extensively (see review in Crossler et al. 2013) to propose numerous models and a wide range of constructs that may possibly influence an individual's decision to adopt or not adopt preventive information security behaviors .This focused primarily on PMT (e.g. Anderson and Agarwal 2010; Herath and Rao 2009; Johnston and Warkentin 2010; Lee and Larsen 2009b; Liang and Xue 2009; Liang and Xue 2010; Siponen et al. 2010), and, to a lesser extent HBM (Davinson and Sillence 2010; Ng et al. 2009). This situation parallels the preventive health behaviors research. As a result, health behavior researchers have called for integration of components from various theories to explain specific behaviors (e.g., Fishbein et al. 2001; Maddux and DuCharme 1997). In so doing, proposed research models can be comprehensive enough to capture a wide range of individual's beliefs regarding their abilities, the existence and seriousness of specific threats, the effectiveness of methods of preventing the threats, and the constraints associated with these methods. PAM responds to this situation by presenting the core constructs, derived from the primary health behavior models and extant IS research, in a comprehensive model of information security behaviors.

The extant research presents several issues to consider regarding the drivers of information security behaviors. First, the theoretical foundation used for these studies varies widely. A number of theories have been proposed as support for the articles' research models, including TPB, HBM, and PMT along with General Deterrence Theory (GDT), Diffusion of Innovation (Rogers 1995), and the Theory of Interpersonal Behavior (Triandis 1980). Also, some researchers have chosen to focus on the effects of these constructs as antecedents to intentions, some directly to behaviors, and others including both. This is consistent with the health behavior literature, since neither HBM nor PMT include intentions directly. This is complicated by varying definitions of intentions/behaviors across papers, and the inclusion of multiple forms of intentions (Anderson and Agarwal 2010) and multiple behaviors (Workman et al. 2008). As a result, the resulting explained variance (R^2) for studies in the information security literature ranges from 0.21-0.78 for intentions and 0.21-0.79 for behaviors.

Over 40 different constructs have been proposed as antecedents to intentions or behaviors. Of these, five constructs are the most common and can be thought to be at the core of security research based on the health behavior models: susceptibility, severity, cost, response efficacy, and self-efficacy. The results for these core constructs alone vary across studies. For instance, response efficacy is significant in 10 studies in which it is measured, while susceptibility has only been found significant in 6 of the 9 studies in which it is measured. Similar inconsistencies exist in the PMT and HBM literature, in which these constructs also vary in significance and effect size (Floyd et al. 2000; Milne et al. 2000; Sheeran and Abraham 1996).

The applicability of these theories to health and security behaviors depends on a set of underlying assumptions that individuals are motivated to perform a preventive action by a desire to avoid or reduce the negative consequences associated with some anticipated event or outcome (Weinstein 1993). This motivation depends upon the individual's assessment of the impact and likelihood of the event and its consequences. The motivation to perform a given action also depends on the individual's belief regarding the effectiveness of the action in reducing its impact or likelihood, and the anticipated barriers to action.

These common assumptions result in a number of conceptually similar, but differently named components which address a common set of antecedents to preventive behavior intentions: impact, likelihood, response efficacy, self-efficacy, and barriers (see Table 1). In HBM and PMT, the impact and likelihood are measured directly as severity and susceptibility, while the individual's belief in the efficacy of the prescribed preventive actions is reflected in the response efficacy (PMT) or perceived benefits (HBM) constructs. In TPB, the assessments of impact, likelihood, and response efficacy are all reflected in the items used to measure individual's attitude toward certain behaviors. With the addition of self-efficacy to revisions of HBM (Sheeran and Abraham 1996) and PMT (Rogers 1983), it is also included in all three

theories. Each theory also includes a measure of the barriers associated with performing a given action. HBM defines this simply as perceived barriers, whereas PMT defines it as response costs along with measures of intrinsic and extrinsic rewards. TPB includes barriers in perceived behavioral control as an external control factor along with other facilitating conditions (Straub and Welke 1998) whereas it includes self-efficacy as an internal control factor.

Table 1: Similar Constructs In Health Behavior Theories and the Preventive Adoption Model

Theory	Impact	Likelihood	Response Efficacy	Self-Efficacy	Barriers	Other
HBM	Severity	Susceptibility	Benefits	Self-efficacy	Cost	Cue to Action
PMT	Severity	Vulnerability	Response Efficacy	Self-efficacy	Cost, intrinsic rewards, extrinsic rewards	
TPB	(Attitude)	(Attitude)	(Attitude)	Perceived Behavioral Control (Self-efficacy)	Perceived Behavioral Control (Facilitating Conditions)	Subjective Norms
PAM	Severity (to Individual, to Organization)	Susceptibility	Avoidability, Response Efficacy	Self-efficacy	Cost, Facilitating Conditions	Cue to Action, Subjective Norms, Ease of Use, Compatibility

Preventive Adoption Model

Leveraging the theories of preventive health behaviors, and consistent with prior research applying these theories to the information security context, we developed the Preventive Adoption Model (PAM). PAM establishes a comprehensive and parsimonious nomology describing the antecedents of individual intentions to engage in preventive information security behaviors. The model integrates constructs from research in preventive health behavior and TPB with other constructs endemic to IS. Specifically, PAM includes severity, susceptibility, avoidability, response efficacy, costs, and cue to action from HBM and PMT. It also includes subjective norms, self-efficacy, and facilitating conditions from TPB, along with ease of use and compatibility from the information systems technology acceptance literature. This integration of constructs is consistent with suggestions from the health behavior literature (e.g., Fishbein et al. 2001; Maddux and DuCharme 1997), while integrating constructs from existing IS literature that are more relevant to the use of preventive information security behaviors. The resulting model is thus more appropriate for explaining individuals' information security behavioral intentions than the health behaviors upon which it is based. The research model guiding our study is shown in Figure 1, along with the origin of the various antecedents. Next, we discuss the constructs and hypothesized relationships which comprise the model.

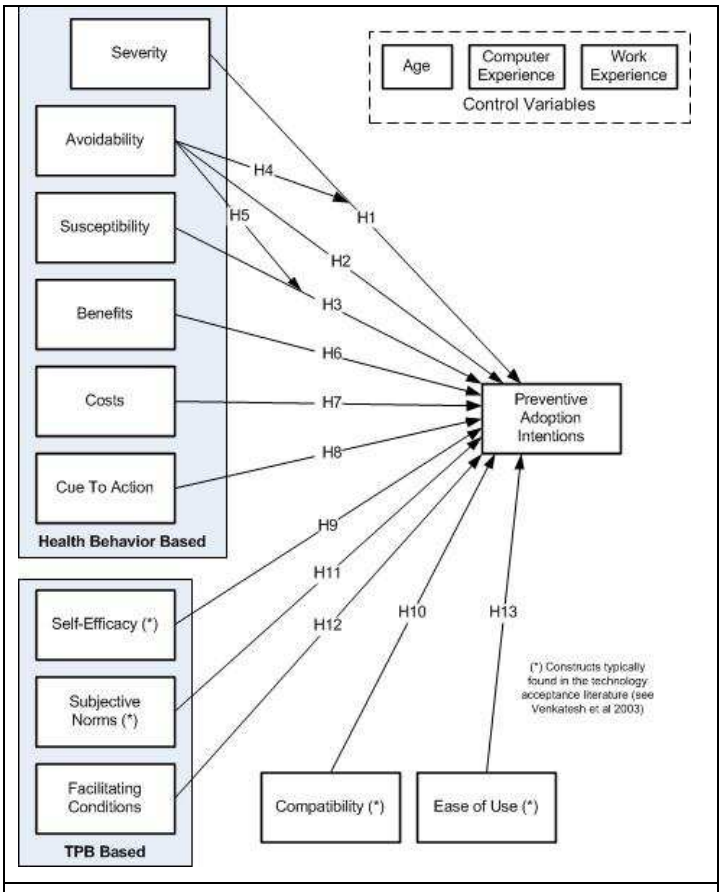

Figure 1. Preventive Adoption Model

Severity

An individual's perceived severity is an assessment of the adverse consequences associated with a given event. This assessment includes not only the technological consequences that may arise (e.g. loss of data, misappropriation of private information), but also psychological, social, or economic consequences (e.g. loss of job, impaired communications). In many cases of an information security problem, the adverse consequences on the organization may be distinctly different from the impact on the individual. The individual's perceptions of the severity to him-/herself and to the organization are two distinctly different, but related, things. As such, severity is conceptualized as a second-order formatively measured construct comprised of two dimensions: an individual's beliefs about the negative impact a security violation would have on the individual, and the impact a security violation would have on the organization in which an individual works. Other contexts may involve additional dimensions (e.g. severity to the customer, to one's home nation, or society as a whole.). However, we have chosen to examine this concept in relation to those factors that are most likely to have an effect on an individual employee's behaviors in an organizational context. Other dimensions may prove to be worth examining in future research studies.

In meta-analyses of HBM (Sheeran and Abraham 1996) and PMT (Milne et al. 2000), perceived severity was found to be among the least-often significant antecedents to intentions or behaviors. However, the extant IS literature has generally found severity to influence intentions (Ifinedo 2012; Komatsu et al. 2013; Siponen et al. 2010). Thus, we hypothesize that as the degree of perceived severity of a given outcome increases, an individual's intentions to exercise behaviors which are likely to prevent the undesirable information security incidents from occurring will increase.

H1: The individual's overall perceived severity of outcomes related to particular security violations are positively associated with the individual's intentions to perform preventive security behaviors.

Susceptibility

Perceived susceptibility is the subjective probability of experiencing a security violation. This probability is manifest in varying degrees, from outright denial that a given computer is susceptible to an information security threat (which is legitimate only for isolated devices not accessible to others or connected to any external data or network) to an irrational over-anticipation of susceptibility (similar to hypochondria in medicine). Individuals' assessments of their susceptibility are often affected by an unrealistic optimism that allows them to conclude that "It won't happen to me" (Weinstein 1984; Weinstein 1987), despite the actual risk. Among other reasons, this bias may be result of a desire to avoid anxiety associated with admitting vulnerability, an effort to maintain one's self-esteem, or cognitive errors such as believing that one is immune to a hazard since it hasn't happened so far (Tversky and Kahneman 1974; Weinstein 1987). The more an individual believes he or she is somehow vulnerable to a given negative outcome, they are more likely to feel it necessary to prevent such behaviors from occurring.

Perceived susceptibility has a mixed review in the health behavior literature, where it has been found to be an often insignificant antecedent of intentions or behaviors in a review of PMT (Milne et al. 2000), but the second most-often significant antecedents in a review of HBM (Sheeran and Abraham 1996). Susceptibility was also found to be an insignificant antecedent in several of the information security behavior articles reviewed. Given the inconsistency of findings, it is possible that susceptibility operates in concert with other factors to influence preventive adoption intentions. Despite the inconsistent findings, the theoretical rationale for the relationship suggests that as perceived susceptibility increases, intentions to do something to prevent the negative outcome from occurring also increase.

H2: An individual's perceived susceptibility to particular security violations is positively associated with intentions to perform preventive security behaviors.

Avoidability

Perceived avoidability is the individual's belief that a security threat can be successfully avoided (Liang and Xue 2010). An information system user's confidence that she can act in ways which may prevent or mitigate a given security violation has a significant effect on their intentions to carry out preventive behaviors. If an individual does not believe that a given negative outcome is avoidable, there is less motivation to carry out the associated preventive security behaviors. As such, perceived avoidability is an indication of the control which users have in determining the outcome of a given threat (Liang and Xue 2009). Thus, higher perceived avoidability increases their intentions to perform the preventive security behaviors.

H3: Higher perceptions of security violation avoidability are positively associated with an individual's intentions to perform preventive security behaviors.

In addition, we propose that perceived avoidability negatively moderates the relationships between a user's perceptions of both severity and susceptibility of potential security violations and the intentions to perform preventive security behaviors. IS users may perceive security risks to be avoidable for a variety of reasons such as lack of experience with certain types of threats, misplaced optimism that "it won't happen to me" (Weinstein 1987), choosing an alternative approach to satisfy system needs, or by enacting specific preventive behaviors. The perception of control to avoid the information security violation undermines assessments of the nature of the threat including minimizing risks associated with a known threat (Liang and Xue 2010; Weinstein 1987). For example, Apple computer users frequently do not install antivirus software even though malware is a known and potentially severe threat (Schofield 2010). Using an alternative computing platform provides means to avoid the potential threat regardless of its prevalence and potential negative consequences. Thus, we posit:

H4: The influence of severity on preventive adoption intentions is negatively moderated by avoidability such that the positive relationship between severity and intentions is weaker the more an individual believes a security violation can be avoided.

H5: The influence of susceptibility on preventive adoption intentions is negatively moderated by avoidability such that the positive relationship between susceptibility and intentions is weaker the more an individual a security violation can be avoided.

Response Efficacy

For the recognition of the severity and susceptibility of a given threat to lead to a change in behaviors, an individual must also believe that their actions will somehow address the threat. Response Efficacy is the individual's beliefs regarding the effectiveness of the alternative responses available for reducing an information security threat. This differs conceptually from the beliefs about avoiding the negative outcomes of a particular threat. Instead, response efficacy (or perceived benefits in HBM) refers to the efficacy of the preventive behaviors themselves, i.e. doing things that keep information security breaches from occurring. These behaviors relate to both the required administrative or operational actions and the act of installing and executing the required technological tools. Previous information security behavior research has typically found response efficacy (or perceived benefits) to be a significant factor in determining intentions and behaviors (e.g., Johnston and Warkentin 2010; Lee and Larsen 2009a). Thus, we propose that the greater the benefits an individual perceives resulting from engaging in preventive security behaviors, the higher the likelihood they will intend to exercise the behaviors.

H6: An individual's perceptions of the response efficacy of preventive behaviors are positively associated with intentions to perform preventive security behaviors.

Costs

The value of the response efficacy is typically weighed against any perceived tangible or psychological costs which may impede the preventive behaviors from being executed. These costs are related to performing the preventive security behaviors, not the costs associated with negative outcomes of an information security breach, which are captured through the individual's perceptions of the severity of a. Costs include the financial resources needed, the time required, and the perceived inconvenience associated with performing the recommended preventive behaviors. As perceived costs increase, an individual is less likely to be motivated to carry out the preventive actions. For example, if expected benefits associated with preventing a given security threat are fully offset or exceeded by the costs of these preventions, an individual is less likely to be motivated to perform the necessary preventive behaviors.

H7: An individual's perceived costs of preventive security behaviors are negatively associated with their intentions to perform preventive security behaviors.

Cue to Action

Cue to action (CTA) is the least studied construct in HBM (Rosenstock et al. 1994) despite anecdotal evidence supporting its importance in stimulating the decision to act upon a given set of beliefs. Salient cues such as expert recommendations, media messages, or experiences (both personal and vicarious) serve as triggers prompting an individual to take the recommended actions (Rosenstock et al. 1994). Though typically cues to action prompt individuals to transform their intentions into actual behavior (Webb and Sheeran 2004), they may also influence the development of intentions to perform the preventive behavior. Such cues, which can include relevant experiences that demonstrate reduced performance or undesirable results associated with an information security failure, influence one's predisposition to perform the behavior in the near future. For example, when a friend shares that his computer was compromised through a Trojan horse and sensitive company information has been accessed (a cue to action), one is more likely to form intentions to keep their antivirus software up to date. Hence, we posit:

H8: Cue to action is positively related to a user's intentions to perform preventive information security behaviors.

Self-Efficacy

Self-efficacy is the individual's belief that he or she is capable of performing the behavior in question. Individuals with high self-efficacy are more likely to persist and to expend more effort in the face of any problems or obstacles that they may encounter (Bandura 1977). Self-efficacy is indicative of an individual's beliefs about their ability to competently perform preventive security behaviors and use preventive security tools (Compeau and Higgins 1995). In the information security behavior literature,

self-efficacy has been found to be significantly associated with both intentions (e.g., Johnston and Warkentin 2010; Liang and Xue 2010) and behaviors (e.g., Ng et al. 2009; Workman et al. 2008). In the health behavior literature, self-efficacy is most often associated with an individual's formation of intentions rather than directly impacting the performance of behaviors directly (Fishbein et al. 2001). This is consistent with the notion that an individual would hardly intend to do something that he or she did not believe they could actually do. Thus, we theorize that higher levels of self-efficacy are associated with increased intentions to perform the given behavior.

H9: Higher self-efficacy is positively associated with the individual's intentions to perform preventive security behaviors.

Compatibility

Compatibility is defined as "the perceived cognitive distance between an innovation and precursor methods for accomplishing tasks." (Rogers 1995, p. 224). In the context of the present study, a compatible preventive information security behavior would fit better with the individual's work practices, thus decreasing the amount of change in one's work practices that is entailed in its enactment. The converse is that some information security practices often have unanticipated consequences which often affect the flexibility and adaptability of both individual and organization (Baskerville 1995). An individual may intend to perform a particular preventive security behavior. However, if the behavior is perceived to be disruptive to normal work patterns and causes significant change to how individuals typically work and to what they can do, these perceived intended and unintended consequences can influence their intentions to engage in such information security behaviors. As such, we hypothesize that compatibility positively affects user intentions to perform preventive security behaviors.

H10: Compatibility of a preventive information security behavior with an individual's work practices is positively associated with the individual's intentions to perform preventive security behaviors.

Subjective Norms, Facilitating Conditions and Ease of Use

The relationships between subjective norms, facilitating conditions and ease of use and intentions have been established in the extant literature. Due to space limitations, the justifications for these hypotheses are not provided but the hypotheses are included for integrity of the nomological network.

H11: Higher levels of perceived normative support are positively associated with an individual's intentions to perform preventive security behaviors.

H12: Higher levels of conditions perceived to facilitate the conduct of preventive security behaviors will be positively associated with an individual's intentions to perform preventive security behaviors.

H13: Perceived ease of use is positively associated with the individual's intentions to perform preventive security behaviors.

Research Methodology

Construct Operationalization

We adapted the majority of our measures from existing validated scales in the health behavior and information security literature. The items for susceptibility, severity, response efficacy, and costs were adapted from a time-tested set of items for HBM (Champion 1984). Items for facilitating conditions and subjective norms were adapted from the corresponding measures in TPB literature (Ajzen 1991). We adapted items from Compeau and Higgins (1995) to measure self-efficacy, and items from Karahanna, Straub, and Chervany (1999) to measure compatibility. Items for ease of use, intentions, and behavior, were based on measures from Davis et al (1989). The specific security behaviors chosen were selected based on a review of the practitioner literature and the results of six semi-structured interviews conducted with both IS and non-IS professional and administrative staff at a large public university in the southern United States. The items for avoidability were developed to be consistent with the conceptual definition as

proposed in Liang and Xue (2009) and in response to their call for development of measures of perceived avoidability (Liang and Xue 2010). The items for cue to action were adapted for the current context from similar measures in the health behavior literature (e.g. Janz and Becker 1984).

We conducted a pilot study to test item wording and online delivery of the survey. The survey was distributed to approximately 100 professionals, working in both IT and non-IT roles, at a large public university in the southern United States. Based on the pilot, we clarified wording of several items and revised the web-based survey to simplify delivery. The full list of items is available upon request.

Severity and preventive adoption intentions are modeled as formatively measured constructs. Understanding these constructs is a primary focus of this study; and this formative modeling allows the constructs to be specified, measured and analyzed more effectively (Petter et al. 2007). Additionally, severity is modeled as a second-order formative construct with two first-order reflective dimensions of severity to the organization and severity to the individual.

A wide variety of information security threats have been the focus of study in the extant literature. For example, Liang and Xue (2010) studied intentions and behaviors associated with spyware, Anderson and Agarwal (2010) assessed security intentions associated with home use of computers and the Internet, and Ng et al (2009) studied security behaviors associated with email usage. Our focus addresses the potential threat of unauthorized access to a workplace computer used for business purposes. The behavioral intentions of interest address separate and distinct actions that individual users may take to protect a work PC from unauthorized access (updating operating system software, using protection software, and logging off the PC when unattended). While not necessarily comprehensive in scope for all organizational users' protection-motivated behaviors (Posey et al. 2013), the measures we have included as formative dimensions are consistent with and adequately capture our context: unauthorized access to a work PC.

The choice to model behavioral intentions and severity as formatively measured constructs also satisfies the decision rules established by Jarvis et al. (2003). First, the direction of causality leads from the underlying dimensions to each construct. For example, changes in severity to the individual would cause severity to change but the reverse may not be the case. Second, the underlying dimensions are not interchangeable as they represent conceptually different aspects of each construct. For example, each preventive adoption action is a separate aspect of the behavioral intention construct – using protection software is not a substitute for logging of an unattended PC. Third, changes in one dimension are not likely to be linked to changes in the other dimensions, i.e., the dimensions should not have substantial covariation. In the case of severity, changes in severity to the organization would not be expected to correlate with changes in individual severity. And lastly, the antecedents and consequents of the dimensions are likely to be different. For instance, individual severity will relate to job specific demands associated with unauthorized access to an employee's work PC whereas organizational severity is likely to reflect liability associated with the consequences of the unauthorized access.

Sample/Data Collection

Survey data were collected from personnel in different business organizations in a major metropolitan area in India. Respondents were working individuals who use a computer as part of their daily job. Working professionals in India were identified as a sample population for testing the research model because India represents an environment where personal computer use in the workplace, while extensive, is much less saturated than in the United States or European countries, and the associated messaging regarding safe computer practices is much less prevalent.

A highly reputable survey panel company located in India collected the data for the study. A total of 2000 employees from a wide-range of companies who use a computer for their work received a paper copy of the survey with a pre-addressed return envelope. The survey was accompanied with a cover letter providing respondents with instructions to complete the survey, as well as a website link which they could use to complete the survey online instead of using the paper survey. Each survey was assigned a unique identification number, thus avoiding the possibility of duplication. Survey participation was encouraged by an optional raffle offering two 10,000 rupees prizes (approximately $220 USD). Survey respondents were guaranteed anonymity and raffle entries were maintained separately from survey response data.

The survey was conducted over a period of 45 days, after which a total of 312 surveys are received. After the initial mailing, a reminder was sent after approximately 25 days. A total of 150 surveys were

completed online and the remaining 162 were received on paper. We received 159 surveys from the initial mailing and 97 following the reminder. We eliminated 38 online surveys due to missing data or inappropriate completion times, resulting in 112 online surveys. Additionally, 18 paper surveys were eliminated for excessive missing data and duplicate responses, resulting in 144 useable paper surveys. The final usable responses were 256, giving a response rate of 12.8%. Descriptive statistics for both formats and the pre- and post-reminder groups, as indicated in Table 2, show no significant differences.

In order to test the responses for non-response bias, early completions are compared against late completions and findings show no significant differences between the two groups.

Table 2. Sample Demographics.

	Online (112)	Paper (144)	Pre-Reminder (159)	Post-Reminder (97)
Age	31.3 years	29.7 years	30.5 yrs	30.2 yrs
Years of Computer Experience	6.9 years	6.3 years	6.6 yrs	6.5 yrs
Years of Total Experience	8.7 years	7.5 years	8.0 yrs	8.0 yrs
Work in IT Dept.	56.7%	47.8%	52.5%	50.5%
Use PC regularly at work	96.2%	97%	97.2%	95.9%
Have internet access at work	99.0%	99.3%	99.3%	68.0%
Position–Sr. Mgr. / Executive	25.0%	20.1%	22.0%	22.7%
Position – Supervisor/ Mgr.	21.4%	16.7%	15.1%	24.7%
Position–Engineer/Tech Spec	34.8%	36.1%	33.3%	39.2%
Position–Analyst/Prof. Staff	10.7%	20.1%	17.6%	12.4%
Position – Admin/Office Staff	5.4%	6.9%	6.3%	6.2%

Analysis and Results

We analyzed the theoretical model using partial least squares (PLS) in SmartPLS 2.0 (M3) Beta (Ringle et al. 2005). Our research model is complex combining a many constructs and structural paths with the second-order construct Severity. PLS is well suited for these complex relationships (Gefen et al. 2011).

Measurement Model Validation

For the reflectively measured constructs, convergent and discriminant validity and reliability tests are used to evaluate the psychometric properties of the measurement model. As shown in Table 6, all scales exhibited adequate reliability with composite reliability scores exceeding the generally accepted guideline of 0.70 and average variance extracted (AVE) exceeding 0.50 (Fornell and Larcker 1981; Nunnally 1978).

To assess the convergent and discriminant validity of the reflective measures, we look for measures to load more on their hypothesized construct than on other constructs (Gefen et al. 2011) and for the square root of AVE to exceed other inter-construct correlations (Chin 2010). Confirmatory factor analysis in PLS should also show item cross-loadings of less than 0.50 (Chin 2010). The measures show adequate convergent and discriminant validity (see Tables 3 and 4).

Table 3. Item Loadings and Cross-Loadings

	Avoid	Comp	Cost	CTA	EOU	FC	REff	SE	SInd	SOrg	SN	SUSC
AVOID1	**0.69**	0.01	0.01	0.08	0.16	0.07	0.23	0.00	0.10	0.27	-0.01	-0.20
AVOID2	**0.80**	-0.07	0.02	0.08	0.26	0.25	0.29	-0.02	0.04	0.34	0.14	-0.03
AVOID3	**0.72**	-0.11	-0.14	-0.07	0.26	0.16	0.30	0.18	0.04	0.19	0.21	-0.09
COMP1	-0.09	**1.00**	-0.51	0.01	-0.21	0.17	0.08	0.09	-0.34	-0.17	-0.03	-0.27
COST1	-0.01	-0.41	**0.86**	0.25	0.05	0.05	0.06	0.06	0.20	0.18	0.07	0.30
COST2	-0.10	-0.40	**0.73**	0.10	-0.13	-0.26	-0.10	-0.09	0.11	0.08	0.00	0.10
CTA_A	0.03	0.01	0.23	**1.00**	-0.04	-0.01	-0.04	0.00	0.13	0.08	0.04	0.20
EOU1	0.28	-0.09	-0.01	0.01	**0.92**	0.23	0.42	0.08	0.17	0.21	0.28	0.00
EOU2	0.26	-0.33	-0.07	-0.09	**0.71**	0.08	0.19	0.09	0.18	0.14	0.23	0.11
FC1	0.15	0.14	-0.15	-0.01	0.29	**0.86**	0.47	0.26	0.13	0.12	0.39	0.01
FC2	0.21	0.13	-0.08	-0.01	0.12	**0.77**	0.40	0.50	0.14	0.17	0.54	-0.17

FC3	0.24	0.15	0.00	0.00	0.06	**0.81**	0.39	0.41	0.09	0.23	0.56	-0.07
RespEff1	0.30	0.21	-0.17	-0.03	0.37	0.32	**0.74**	0.24	0.01	0.32	0.25	-0.10
RespEff2	0.21	-0.10	-0.06	-0.11	0.37	0.31	**0.62**	0.41	0.17	0.25	0.36	0.08
RespEff3	0.29	0.02	0.15	0.00	0.20	0.49	**0.83**	0.39	0.10	0.22	0.44	-0.03
SE1	0.05	0.09	0.02	0.02	0.06	0.35	0.39	**0.97**	0.01	0.18	0.41	0.00
SE2	0.16	0.05	-0.09	-0.03	0.17	0.53	0.46	**0.75**	0.19	0.20	0.62	0.03
SInd1	0.04	-0.22	0.12	0.13	0.08	0.07	0.04	0.02	**0.78**	0.31	0.14	0.27
SInd2	0.08	-0.38	0.16	0.09	0.23	0.12	0.09	0.06	**0.84**	0.42	0.20	0.27
SInd3	0.06	-0.24	0.20	0.11	0.19	0.16	0.13	0.05	**0.87**	0.42	0.29	0.37
SOrg1	0.22	-0.09	0.22	0.15	0.16	0.16	0.22	0.06	0.36	**0.72**	0.15	0.12
SOrg2	0.25	-0.17	0.12	0.07	0.24	0.24	0.31	0.16	0.37	**0.82**	0.31	0.11
SOrg3	0.38	-0.08	-0.01	0.05	0.24	0.16	0.29	0.15	0.38	**0.77**	0.30	0.14
SOrg4	0.24	-0.19	0.21	-0.02	0.02	0.07	0.24	0.25	0.32	**0.77**	0.23	0.10
SN1	0.20	0.00	0.04	0.07	0.29	0.56	0.44	0.46	0.19	0.29	**0.95**	0.07
SN2	0.09	-0.08	0.06	-0.03	0.25	0.46	0.40	0.46	0.33	0.29	**0.82**	0.01
SUSC1	-0.12	-0.27	0.26	0.20	0.05	-0.06	-0.04	0.00	0.37	0.16	0.05	**1.00**

Notes: Avoid=Avoidability; Comp=Compatibility; CTA=Cue-to-Action; EOU=Ease of Use; FC=Facilitating Conditions; RespEff=Response Efficacy; SE=Self Efficacy; SInd=Severity to Individual; SOrg=Severity to Organization; SUSC=Susceptibility; SN=Subjective Norms

Three of the constructs in the study were based on single item measures, an acknowledged limitation. Cue-to-Action (CTA) used the average of responses to 3 dichotomous questions asking if the respondent had experienced particular cues in the past year (i.e., heard news about dangers of, someone known had experienced, and personally experienced unauthorized access). Both compatibility and susceptibility were originally modeled with two items, and in each case, an item was dropped for statistical reasons.

The traditional methods of assessing validity for reflective measures are not appropriate for formative measures (Jarvis et al. 2003; Petter et al. 2007; Roberts and Thatcher 2009). The first need is to establish the content validity of the items used to capture the domain of the construct (Straub et al. 2004). The items should represent a consensus covering the scope of the construct (Roberts and Thatcher 2009). The items, as derived from the practitioner literature and interviews, identify the actions individuals are most commonly encouraged to take to promote information security by preventing unauthorized access to their work PC. The items were refined through the pilot study and adequately represent the construct domain.

Table 4. Inter-construct Correlations and Composite Reliability

Constructs	CR (# items)	Avoid	Comp	Cost	CTA	EOU	FC	Resp Eff	SE
Avoidability	0.78 (3)	**0.74**							
Compatibility	n/a (1)	-0.09	**n/a**						
Cost	0.78 (2)	-0.06	-0.51	**0.80**					
Cue-to-Action	n/a (1)	0.03	0.01	0.23	**n/a**				
Ease of Use	0.81 (2)	0.32	-0.21	-0.03	-0.04	**0.82**			
Fac. Cond.	0.85 (3)	0.23	0.17	-0.10	-0.01	0.21	**0.82**		
Resp. Efficacy	0.78 (3)	0.37	0.08	-0.01	-0.04	0.40	0.52	**0.73**	
Self Efficacy	0.86 (2)	0.08	0.09	-0.01	0.00	0.10	0.43	0.45	**0.87**
Severity_Ind	0.87 (3)	0.07	-0.34	0.20	0.13	0.21	0.14	0.11	0.06
Severity_Org	0.85 (4)	0.36	-0.17	0.17	0.08	0.22	0.21	0.35	0.20
Susceptibility	n/a (1)	-0.12	-0.27	0.26	0.20	0.05	-0.06	-0.04	0.00
Subjective Norm	0.88 (2)	0.18	-0.03	0.05	0.04	0.31	0.58	0.47	0.50
Intentions1	**n/a**	0.11	-0.14	0.29	0.08	0.12	0.15	0.22	0.06
Intentions2	**n/a**	0.17	-0.14	0.23	0.05	0.29	0.15	0.34	0.05
Intentions3	**n/a**	0.29	0.12	-0.12	-0.09	0.24	0.16	0.26	0.13

	Sev_I	Sev_O	Susc	SN
Severity_Ind	**0.83**			
Severity_Org	0.47	**0.77**		
Susceptibility	0.37	0.16	**n/a**	
Subjective Norm	0.26	0.32	0.05	**0.89**
Intentions1	0.32	0.44	0.32	0.27
Intentions2	0.25	0.41	0.35	0.26
Intentions3	-0.04	-0.02	-0.07	0.17

To establish evidence of construct validity, indicator weights, indicator loadings and absence of multicollinearity were evaluated (Cenfetelli and Bassellier 2009; Petter et al. 2007). Item loadings and weights for the formative constructs are shown in Table 5. The results indicate both absolute and relative importance for INT2, and absolute importance for INT1, and lack of absolute and relative importance for INT3 (Cenfetelli and Bassellier 2009). However, when an item lacks both absolute and relative importance in a statistical sense, the determination to maintain the formative item shifts to the theoretical relevance of the item. These three items represent fundamentally distinct security prevention behaviors that are not interchangeable. All three items were included as maintaining the content validity of the formative construct holds greater influence than the statistical results (Petter et al. 2007). We view all three items as integral components of intended security behaviors. The variance inflation factor (VIF) was used to evaluate multicollinearity. The VIF values were less than 2.07 for the intention items, below the suggested threshold of 3.3 (Petter et al. 2007), thus demonstrating that multicollinearity is not a threat.

Table 5. Outer Model Weights and Loadings

Item	Item Weights	Standard Error	T-Statistic	Item Loadings	Standard Error	T-Statistic
INT1	0.238	0.224	1.061	0.814	0.181	4.511
INT2	0.798	0.158	5.052	0.973	0.108	9.069
INT3	0.143	0.185	0.770	0.175	0.221	0.794

Severity was modeled as a second-order formative construct with severity to the individual and severity to the organization as its underlying dimensions. The paths of the underlying dimensions are both significant as are five of the seven path weights of the individual indicators on the second order construct. Per the recommendations of Wetzels et al. (2009), we conclude that severity is appropriately modeled.

As with all research using self-reported data and all construct variables being measured through the same survey instrument, common method bias is a potential (Podsakoff et al. 2003). Several steps were taken to mitigate these concerns: the measures for the exogenous variables were separated in the survey from those for the endogenous constructs (Salancik and Pfeffer 1977); the survey was administered in two different forms with approximately half taking the survey online and half completing a paper-based version; and the survey started with a statement that the questions had no right or wrong answers so respondents could answer honestly, and that anonymity was assured (Podsakoff et al 2003). A post hoc statistical analysis to assess the presence of common method bias (i.e. Harman's one-factor test) identified seven factors with the largest accounting for less than 25 percent of variance explained which is substantially below the 50 percent threshold, thus indicating common method bias is not a concern. Additionally, item level t-test comparisons between online and paper responses indicate no differences further minimizing method bias concerns.

Structural Model Testing

The full model was tested in PLS. The results are presented in Figure 2. The PAM model accounts for 56 percent of the variance in preventive security behavior intentions. This demonstrates adequate explanatory power of the model (Hair et al. 1998). The results of the hypotheses tests are presented in Table 6 and show support for eight of the thirteen hypotheses. A post hoc statistical testing using G*Power 3.1 (Faul et al. 2007) estimates a statistical power exceeding 0.99.

The results are robust after controlling for age, computer experience and work experience. Age and work experience had no effect on preventive security behavior intentions. Computer experience influenced intentions such that more experienced computer users demonstrated lower intentions to engage in preventive security behaviors.

The proposed interaction effects were evaluated using the product-indicator approach (Chin et al. 2003; Henseler et al. 2010). To reduce multicollinearity, the items were standardized prior to multiplication (Aiken et al. 1991). The interaction between avoidability and susceptibility is significant ($b = -.22$, $p<0.01$) as is the interaction between avoidability and severity ($b = -.32$, $p<0.10$). To evaluate the moderation effects, the effect size (f^2) of the moderations was calculated by comparing R^2 values between the main effects model and models with the moderations (Chin et al. 2003). We calculated f^2 (see Table 7) for models with both interaction terms as well as each interaction term separately. These results provide

strong support for hypotheses H4 and H5.

Table 6. Results by Hypotheses		
Hypothesis	**Support?**	**Path/t-value/ Significance**
H1: Severity → Preventive Security Behavior Intentions	No	n.s.
H2: Susceptibility → Preventive Security Behavior Intentions	Yes	β=0.29, t= 4.12, p<.001
H3: Avoidability → Preventive Security Behavior Intentions	Yes	β=0.15, t=1.90, p<.05
H4: Avoidability moderates Severity → Intentions	Yes	β= -0.32, t=1.43, p<.10
H5: Avoidability moderates Susceptibility → Intentions	Yes	β= -0.22, t=3.08, p<.01
H6: Response Efficacy → Preventive Security Behavior Intentions	Yes	β=0.22, t=2.95, p<.01
H7: Costs → Preventive Security Behavior Intentions	No	β=0.19, t=2.46, p<.01
H8: Cue-to-Action → Preventive Security Behavior Intentions	No	n.s.
H9: Self Efficacy → Preventive Security Behavior Intentions	No	n.s.
H10: Subjective Norms → Preventive Security Behavior Intentions	Yes	β=0.11, t=1.35, p<.10
H11: Fac Conditions → Preventive Security Behavior Intentions	No	n.s.
H12: Compatibility → Preventive Security Behavior Intentions	Yes	β=0.09, t=1.51, p<.10
H13: Ease of Use → Preventive Security Behavior Intentions	Yes	β=0.14, t=2.06, p<.05

Table 7. Interaction Effect Size			
Interaction Terms	**R^2 (Intentions)**	**Effect Size (f^2)[1]**	**Magnitude**
Both	0.56	0.33	Medium-Large
Avoidance x Severity	0.52	0.24	Medium-Large
Avoidance x Susceptibility	0.48	0.14	Small-Med
Base Model	*0.42*	--	--

Discussion and Implications

This study proposes and empirically tests the Preventive Adoption Model (PAM). The extant IS literature shows a growing consensus that health behavior models offer many potential insights into the motivations driving information security behaviors. PAM integrates three health behavior theories (Health Belief Model, Prevention Motivation Theory, and the Theory of Planned Behavior) into a comprehensive yet parsimonious model for understanding the primary antecedents of preventive adoption intentions. The empirical test provides strong support for PAM in the study context, explaining 56 percent of the variance in intentions to perform security behaviors associated with preventing unauthorized access.

Based on a sample of 237, eight of the thirteen hypotheses in PAM were supported. Specifically, as hypothesized, intentions to engage in preventive security behaviors are influenced by several constructs derived from the health behavior literature (perceived susceptibility, avoidability, response efficacy), the technology acceptance literature (ease of use, subjective norm, and compatibility), and the theory of planned behavior (subjective norms and compatibility).

The direct relationship between severity and intentions (H1) was not significant. However, there was a significant moderating effect of avoidability on the relationship between severity and intentions (H4). The interaction graph (excluded for space considerations) indicates that when consequences are severe, people intend to engage in preventive security behaviors irrespective of level of avoidability. When consequences are low in severity, the level of avoidability determines the extent to which people intend to engage in security behaviors. Avoidability also had a significant moderating effect on the relationship between susceptibility and intentions (H5). This interaction graph suggests that when avoidability is high people intend to engage in preventive security behaviors irrespective of level of susceptibility. However

[1] f^2 is calculated as: [R^2 (Interaction Model)–R^2 (Main Effects Model)]/[1 – R^2 (Main Effects Model)]. For f^2, values of 0.02, 0.15, and 0.35 are considered to be small, medium, and large effect sizes respectively (Chin et al 2003).

when avoidability is low peoples' intentions increase as level of susceptibility increases.

The hypothesized relationship self-efficacy on preventive adoption intentions (H9) was not significant. A possible explanation may lie in the specific items used to measure self-efficacy. Our items captured the individual's confidence relative to a general level of performing generic security behaviors as opposed to capturing self-efficacy with respect to specific behaviors related to preventing unauthorized access.

The relationship between facilitating conditions and intentions (H12) was not supported. This indicates that the subjects were not influenced by the existence or non-existence of the necessary conditions for engaging in preventive behaviors. This may suggest that the security related software, tools, and support available are not viewed as enablers or obstacles because of their widespread availability. Perceived cost was found to be significant, but with the opposite influence than was hypothesized, and thus H7 is not supported. This is not surprising, since hypotheses for perceived costs are frequently not supported within health behavior literature. It is also possible that the subjects are exhibiting psychological pricing (Kotler 2003), in which customers use price or cost of a product or service as an indicator of quality (Erickson et al. 1985; Rao et al. 1989). Our subjects seem to assume that the higher the costs, the more effective the preventive behaviors. Finally, cue to action (H8) was not significant, which was not surprising based on inconsistent results from the HBM literature. Although the items included in the survey were tested in a pilot study and are consistent with previous research, we may not have captured the full range of possible cues sufficient to encourage the corresponding behaviors by the study participants. It is also possible that cues to action influence the enactment of behavior directly by prompting individuals to spring to action rather than influence the formation of behavior intentions.

There are a number of limitations in this study that should be acknowledged. First, the data was collected based on a sample of professionals in India. While the language of daily business discourse is English, and efforts were made to ensure the survey verbiage utilized appropriate and generally accepted terminology, it is possible the findings have been influenced by culturally-based interpretations. Thus, care need be taken before generalizing the findings to other populations. Future research should replicate testing of PAM using both business and non-business computer users in a variety of cultural settings.

Second, research suggests that individuals will respond to general information security threats, such as unauthorized access to a work computer, differently than to specific, single focused threats (e.g. viruses, hacks, or phishing/spam). We focused on behavioral intentions dealing with the more general conceptualization of threat of unauthorized access to one's computer. Greater insights may be gained by incorporating a variety of information security threats and behavior-coping strategies into PAM.

Lastly, cue to action (CTA) was calculated as the average of three dichotomous indicators. Several factors could influence the extent to which various cues actually motivate preventive behavior intentions that may be obscured by our measure. We used a timeframe of one year for a cue. More timely cues may actually exert greater influence. The consequences faced by others acting as a cue to action may also determine the strength of the prompt. Our measures focused on only negative consequences from unauthorized access. Different situational cues may influence individuals to either engage in cognitive decision making processes or to engage in specific behaviors (Maddux et al. 1997). Future research should seek to clarify the existence and impact of situational cues to action, and cues to action incorporating different timeframes, a variety of cueing mechanisms, and both positive and negative prompts.

Recent IS research has proposed higher order constructs such as perceived threat and security related attitude as mediators of behavior intentions (Anderson et al. 2010; Liang et al. 2010). While beneficial, these approaches may obscure the unique influences of the primary antecedents of behavioral intentions. PAM adopts the approach most common in health behavior research to model the influence of key antecedents as direct relationships to behavioral intentions.

Direct modeling of the antecedents to intentions in PAM is also important for evaluating the potential for moderations influencing assessments of severity and susceptibility drawn from HBM and PMT. Liang and Xue (2010) demonstrated a counter-intuitive negative moderation of threat and response efficacy on intentions. We have confirmed this finding and further clarified that both perceived susceptibility and perceived severity are negatively moderated by perceptions that security issues are avoidable. In essence, perceived susceptibility and avoidability are separate and distinct influences on intentions. Individuals may see that certain threats are avoidable, either by adopting specific preventive behaviors or by finding alternative methods to achieve the desired computer functions.

Conclusions

This study sought to develop a model to examine organizational users' preventive adoption of information security behaviors, based on similar models in the health behavior literature. The resulting model was derived by integrating concepts from the health belief model, protection motivation theory, and theory of planned behavior, along with other constructs specific to the information systems and information security contexts. The results of the study provide strong support for the Preventive Adoption Model with high explained variance in preventive security intentions. The results also show that users' beliefs regarding the threat and its avoidability, the outcome of the prescribed preventive behaviors, and the compatibility between these behaviors and the users' work roles and responsibilities are key factors in determining users' intentions to practice information security behaviors.

References

Aiken, L.S., and West, S.G. 1991. *Multiple Regression: Testing and Interpreting Interactions*. Newbury Park, CA: Sage.

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

Anderson, C., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.

Bandura, A. 1977. *Social Learning Theory*. New York: General Learning Press.

Baskerville, R. 1995. "The Second Order Security Dilemma," *IFIP WG8.2 Working Conference on Information Technology and Changes in Organizational Work,* W. Orlikowski (ed.): Springer, pp. 239-249.

Cenfetelli, R.T., and Bassellier, G. 2009. "Interpretation of Formative Measurement in Information Systems Research," *MIS Quarterly* (33:4), pp. 689-707.

Champion, V. 1984. "Instrument Development for Health Belief Model Constructs," *Advances in Nursing Science* (6:3), pp. 73-85.

Chin, W. 2010. "How to Write up and Report Pls Analyses," in *Handbook of Partial Least Squares,* V.V. Esposito (ed.). Verlag Berlin Heidelberg: Springer, pp. 655-690.

Chin, W.W., Marcolin, B.L., and Newsted, P.R. 2003. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Studyand an Electronic Mail Adoption Study," *Information Systems Research* (14:2), pp. 189-217.

Compeau, D., and Higgins, C.A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), pp. 189-211.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), February, pp. 90-101.

D'Arcy, J., Hovav, A., and Galletta, D.F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Davinson, N., and Sillence, E. 2010. "It Won't Happen to Me: Promoting Secure Behaviour among Internet Users," *Computers in Human Behavior* (26:6), pp. 1739-1747.

Davis, F.D., Bagozzi, R.P., and Warshaw, P. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 982-1003.

Erickson, G.M., and Johansson, J.K. 1985. "The Role of Price in Multi-Attribute Product Evaluations," *Journal of Consumer Research* (12:2), pp. 195-199.

Faul, F., Erdfelder, E., Lang, A.-G., and Buchner, A. 2007. "G*Power 3: A Flexible Statistical Power Analysis Program for the Social, Behavioral, and Biomedical Sciences," *Behavior Research Methods* (39), pp. 175-191.

Fishbein, M., Triandis, H.C., Kanfer, F.H., Becker, M., Middlestadt, S.E., and Eichler, A. 2001. "Factors Influencing Behavior and Behavior Change," in *Handbook of Health Psychology,* A. Baum, T. Revenson and J. Singer (eds.). Hillsdale, NJ: Lawrence Erlbaum.

Floyd, D., Prentice-Dunn, S., and Rogers, R.W. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 407-429.

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

Gefen, D., Rigdon, E.E., and Straub, D. 2011. "An Update and Extension to Sem Guidelines for Administrative and Social Science Research," *MIS Quarterly* (35:2), pp. iii-xiv.

Glanz, K., Rimer, B.K., and Viswanath, K. 2008. *Health Behavior and Health Education: Theory, Research, and Practice*. San Francisco: Jossey-Bass.

Hair, J.F., Tatham, R.L., Anderson, R.E., and Black, W. 1998. *Multivariate Data Analysis (5th Edition)*, (5th ed.). New Jersey: Prentice Hall.

Henseler, J., and Fassott, G. 2010. "Testing Moderating Effects in Pls Path Models: An Illustration of Available Procedures," in *Handbook of Partial Least Squares,* V.E. Vinzi, W.W. Chin, J. Henseler and H. Wang (eds.). New York: Springer, pp. 713-735.

Herath, T., and Rao, H.R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," *European Journal of Information Systems* (18:2), pp. 106-125.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31), pp. 83-95.

Janz, N.K., and Becker, M.H. 1984. "The Health Belief Model: A Decade Later," Health Education Quarterly (11:1), Spring, pp. 1-47.

Jarvis, C.B., Mackenzie, S.B., 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), September, pp. 199-218.

Johnston, A.C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:2), pp. 1-xxx.

Karahanna, E., Straub, D.W., and Chervany, N.L. 1999. "Information Technology Adoption across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs," in: *MIS Quarterly*. pp. 183-213.

Komatsu, A., Takagi, D., and Takemura, T. 2013. "Human Aspects of Information Security," *Information Management & Computer Security* (21:1), pp. 5-15.

Kotler, P. 2003. *Marketing Management*, (11th ed. ed.). New York: Prentice Hall.

Lee, Y., and Larsen, K. 2009a. "Threat or Coping Apprisal: Seterminants of Smb Executives' Decision to Adopt Ati-Malware Software," *European Journal of Information Systems* (18:2), pp. 177-187.

Lee, Y., and Larsen, K.R. 2009b. "Threat or Coping Appraisal: Determinants of Smb Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18:2), pp. 177-187.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71-90.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Maddux, J.E., and DuCharme, K. 1997. "Behavioral Intentions in Theories of Health Behavior," in *Handbook of Health Behavior Research I: Personal and Social Determinants,* D. Gochman (ed.). New York: Plenum Press, pp. 133-151.

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

Ng, B.-Y., Kankanhalli, A., and Xu, Y. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46), pp. 815-825.

Ng, B.-Y., and Xu, Y. 2009. "Studying Users' Computer Security Behavior Using the Health Belief Model," *11th Pacific-Asia Conference on Information Systems*, Auckland, New Zealand, pp. 423-437.

Nunnally, J.C. 1978. *Psychometric Theory*. New York: McGraw-Hill.

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

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y. L., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," Journal of Applied Psychology (88:5), pp 879-903.

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

Prentice-Dunn, S., and Rogers, R.W. 1986. "Protection Motivation Theory and Preventive Health: Beyond

the Health Belief Model," *Health Education Research* (1), pp. 153-161.
Rao, A.R., and Monroe, K.B. 1989. "The Effect of Price, Brand Name, and Store Name on Buyers' Perceptions of Product Quality: An Integrative Review," *Journal of Marketing Research* (26:3), pp. 351-357.
Ringle, C.M., Wende, S., and Will, A. 2005. "Smartpls, Version 2.0 Beta." Hamburg, Germany: University of Hamburg.
Roberts, N., and Thatcher, J.B. 2009. "Conceptualizing and Testing Formative Constructs: Tutorial and Annotated Example," *The DATA BASE for Advances in Information Systems* (40:3), pp. 9-39.
Rogers, E.M. 1995. *Diffusion of Innovations*, (Fourth Edition ed.). New York: The Free Press.
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 Protection Motivation. ," in *Social Psychophysiology,* J. Cacioppo and R. Petty (eds.). New York: Guilford Press.
Rosenstock, I.M. 1966. "Why People Use Health Services," *Milbank Memorial Fund Quarterly* (XLIV:3), July 1966, pp. 94-124.
Rosenstock, I.M. 1974. "The Health Belief Model and Preventive Health Behavior," *Health Education Monographs* (2:4), Winter 1974, pp. 354-386.
Rosenstock, I.M., Strecher, V., and Becker, M. 1994. "The Health Belief Model and Hiv Risk Behavior Change," in *Preventing Aids: Theory and Practice of Behavioral Interventions,* J. Peterson and R. DiClemente (eds.). New York: Plenum Press.
Salancik, G.R., and Pfeffer, J. 1977. "An Examination of Need-Satisfaction Models of Job Attitudes," *Administrative Science Quarterly* (22:3), September, pp. 427-456.
Schofield, J. 2010. "Does a Mac Need Anti-Virus Protection?" Retrieved January 19, 2011, from http://www.guardian.co.uk/technology/askjack/2010/feb/03/apple-data-computer-security
Sheeran, P., and Abraham, C. 1996. "The Health Belief Model," in *Predicting Health Behavior,* M. Conner and P. Norman (eds.). Buckingham: Open University Press, pp. 23-61.
Siponen, M., Pahnila, S., and Mahmood, A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *IEEE Computer* (43:10), pp. 64-71.
Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information System Security Policy Violation," *MIS Quarterly* (34:3), pp. 487-502.
Straub, D.W. 1990. "Effective Is Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.
Straub, D.W., Boudreau, M.-C., and Gefen, D. 2004. "Validation Guidelines for Is Positivist Research," *Communications of the AIS* (14), pp. 380-426.
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.
Triandis, H.C. 1980. "Values, Attitudes, and Interpersonal Behavior," in *Nebraska Symposium on Motivation, 1979,* H. Howe and M. Page (eds.). Lincoln: University of Nebraska Press, pp. 196-259.
Tversky, A., and Kahneman, D. 1974. "Judgment under Uncertainty: Heuristics and Biases," *Science* (185:4157), pp. 1124-1131.
Von Solms, B. 2001. "Information Security - a Multidimensional Discipline," *Computers & Security* (20:6), pp. 504-508.
Webb, T., and Sheeran, P. 2004. "Identifying Good Opportunites to Act: Implementation Intentions and Cue Discrimination," *European Journal of Social Psychology* (34), pp. 407-419.
Weinstein, N.D. 1984. "Why It Won't Happen to Me: Perceptions of Risk Factors and Susceptibility," *Health Psychology* (3:5), pp. 431-457.
Wetzels, M., Odekerken-Schröder, G., and van Oppen, C. 2009. "Using Pls Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration," *MIS Quarterly* (33:1), March, pp. 177-195.
Whitehouse, S., Mikulsky, B., and Snowe, O. 2010. "Cyber Self-Defense Can Help U.S. Security (9/3/2010)," in: *CNN.com*.
Workman, M., Bommer, W.H., and Straub, D. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Health Behavior* (24), pp. 2799-2816.