Research Article

Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective*

Huigang Liang
East Carolina University
huigang.liang@gmail.com

Yajiong Xue
East Carolina University
yajiong.xue@gmail.com

Abstract

This study aims to understand the IT threat avoidance behaviors of personal computer users. We tested a research model derived from Technology Threat Avoidance Theory (TTAT) using survey data. We find that users' IT threat avoidance behavior is predicted by avoidance motivation, which, in turn, is determined by perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy. Users develop a threat perception when they believe that the malicious IT is likely to attack them (perceived susceptibility) and the negative consequences will be severe if they are attacked (perceived severity). When threatened, users are more motivated to avoid the threat if they believe that the safeguarding measure is effective (safeguard effectiveness) and inexpensive (safeguard cost) and they have confidence in using it (self-efficacy). In addition, we find that perceived threat and safeguard effectiveness have a negative interaction on avoidance motivation so that a higher level of perceived threat is associated with a weaker relationship between safeguard effectiveness and avoidance motivation or a higher level of safeguard effectiveness is associated with a weaker relationship between perceived threat and avoidance motivation. These findings provide an enriched understanding about personal computer users' IT threat avoidance behavior.

Keywords: *threat, avoidance, susceptibility, severity, safeguarding measure, motivation, security, home setting*

* Dennis Galletta was the accepting senior editor. This was submitted on March 24, 2009 and went through two revisions.

Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective

1. Introduction

In this information era, the use of personal computers and the Internet is widely diffused. The US Census Bureau reported that 62 percent of American households owned a computer and 55 percent had Internet access in 2003 (Day et al., 2005). The latest Pew/Internet survey shows that 74 percent of American adults and 93 percent of teenagers have Internet access at home (Jones and Fox, 2009). Equipped with the Internet, personal computers are now an important virtual setting for everyday living and work. A wide range of mundane activities such as shopping, chatting, socializing, reading, entertaining, and banking can be done on personal computers. In addition, as organizations have become increasingly virtualized, work is transcending physical restrictions (Handy, 1995). Employees can choose to work at home or bring unfinished work to their homes because Internet technologies allow them to turn their personal computers into virtual offices. The boundary between work and life has been remarkably blurred. Despite the importance of personal computer use, individual users are particularly vulnerable to IT threats. Unlike employees in organizations and companies, these users do not have to comply with strict IT security policies and it is unlikely that they have strong IT security infrastructure to protect them from malware and hackers. For example, most home users are not computer professionals and lack the expertise to set up a safe home computing system. In addition, unsafe computing behaviors of naïve home users — such as browsing unsafe websites, downloading suspicious software, sharing passwords with family members, and not protecting home wireless networks — expose home computers to many lurking dangers.

Given the pervasiveness of personal computer and Internet use and the blurred line between work and home, IT security breaches on personal computers can cause damages not only to individuals, but also to organizations. On the one hand, users may become victim to identity theft if their personal information is stolen. On the other hand, users' unsafe computing behavior in non-work settings may open a "back door" for hackers to break into their companies' systems. For example, when a user logs into his or her company's intranet from home, hackers can use Trojan to steal the password and use it to illegally access the company's confidential data. Cyber criminals can also turn numerous weakly secured home computers into Zombie computers and use them to create botnets to attack other personal computers and corporate applications. The diffusion of the Internet has made it easy for malicious IT to exploit system vulnerabilities and amplify the negative impact. Many forms of malicious IT such as viruses, worms, spyware, Trojan horses, and botnets have caused enormous financial losses (Bagchi and Udo, 2003). As the CSI survey shows, in 2009, 64.3 percent of the responding organizations were attacked by malware, and security problems resulted in an average loss of over $234,244 per organization (CSI, 2009). Consumer Reports' "State of the Net" survey indicates that in a two-year period from 2007 to 2009, the financial losses of U.S. consumers due to viruses and spyware were $5.8 billion and $1.7 billion, respectively (Consumer Reports, 2009). Given its huge economic impact, IT security has drawn great attention from information systems (IS) researchers and practitioners (Baskerville, 1993; Dhillon and Backhouse, 2000; Loch et al., 1992). However, most prior research on IT security has been conducted in organizational settings (D'Arcy et al., 2009; Straub and Welke, 1998), and little is known about user security behavior in the context of personal computer use.

Researchers have recently noticed that technology alone is insufficient to ensure security and have started to pay attention to the human aspect of security (Anderson and Agarwal, 2006; Aytes and Terry, 2004; Ng et al., 2009; Woon et al., 2005; Workman et al., 2008). Yet, knowledge about user security behaviors is far from complete. The purpose of this study is to investigate how personal computer users cope with IT threats. We derive a research model from Technology Threat Avoidance Theory (TTAT; Liang and Xue, 2009) to explain how individuals develop threat perceptions, evaluate safeguard measures, and engage in avoidance behavior. Our empirical results provide strong support for our research model.

This paper makes several contributions to the IS literature. First, as one of the first attempts to empirically validate TTAT, it investigates an important phenomenon – the security behavior of personal computer users – that is vaguely understood. Our study shows that users are motivated to perform security behaviors if they perceive the threat to be present and avoidable. Second, it shows

that both perceived susceptibility and severity of the negative consequences caused by malicious IT motivate users to avoid the IT threat, and their effects are fully mediated by the threat perception. This finding helps to clarify the threat assessment, about which prior studies on IT security have generated inconsistent findings (Ng et al., 2009; Woon et al., 2005; Workman et al., 2008). Finally, our study reveals a counterintuitive finding – perceived threat and safeguard effectiveness have a negative interaction when they influence avoidance motivation, which has not been reported in empirical studies.

The paper proceeds as follows. We first discuss the theoretical foundation and then describe our research model and hypotheses. Then, we present our methodology, followed by data analysis results. In the discussion section, we highlight major findings and provide implications for research and practice. After discussing limitations and future research directions, we end the paper with a brief conclusion.

2. Theoretical Foundation

This study is grounded on TTAT, which explains why and how individuals avoid IT threats in voluntary settings (Liang and Xue, 2009). Liang and Xue developed TTAT by synthesizing the literature from a range of areas including psychology, health care, risk analysis, and IS. The basic premise of TTAT is that when users perceive an IT threat, they are motivated to actively avoid the threat by taking a safeguarding measure if they perceive the threat to be avoidable by the safeguarding measure, and they may also passively avoid the threat by performing emotion-focused coping.

TTAT delineates the process and the factors that influence IT users' threat avoidance behavior (Liang and Xue, 2009). It posits that IT threat avoidance behavior can be depicted as a cybernetic process in which users aim to enlarge the distance between their current security state and the unsafe end state (Carver and Scheier, 1982; Edwards, 1992). Users first appraise the existence and degree of the IT threat that they are facing and then assess what they can do to avoid the threat (Lazarus, 1966; Lazarus and Folkman, 1984). Based on these appraisals, they decide which safeguarding measure to use to reduce the threat. A set of key factors have been identified to reflect user perceptions, motivations, and behaviors during this process. According to TTAT, users will avoid a malicious IT if they believe that the malicious IT is a threat and can be avoided by applying a safeguard. Integrating research into risk analysis (Baskerville, 1991a; Baskerville, 1991b) and health psychology (Janz and Becker, 1984; Rogers, 1983; Weinstein, 2000), TTAT proposes that users' threat perceptions are determined by the perceived probability of the threat's occurrence and the perceived severity of the threat's negative consequences. Following prior research on health protective behavior (Janz and Becker, 1984; Maddus and Rogers, 1983) and self-efficacy (Bandura, 1982; Compeau and Higgins, 1995), TTAT submits that users consider three factors to evaluate how avoidable the threat is if they take a safeguarding measure – the effectiveness of the safeguard, the costs of the safeguard, and user self-efficacy of applying the safeguard.

TTAT develops a general theoretical framework within which users' security behaviors can be explained. It is especially useful for explaining voluntary security behaviors in non-work settings where IT security is not mandated. Therefore, we believe TTAT is an appropriate to investigate personal computer users' IT security behavior.

3. Research Model and Hypotheses

We derive a research model (Figure 1) from the variance model of TTAT (Liang and Xue, 2009) to examine how users avoid IT threats by using a given safeguarding measure. Consistent with TTAT, we propose that users' IT threat avoidance behavior is determined by avoidance motivation, which, in turn, is affected by perceived threat. Perceived threat is influenced by perceived severity and susceptibility as well as their interaction. While the original TTAT suggests that the effects of safeguard effectiveness, safeguard cost, and self-efficacy are mediated by perceived avoidability, in this research we propose that avoidance motivation is directly determined by the three constructs. This change allows us to precisely delineate the direct effects of these constructs, in case perceived avoidablity cannot fully mediate these effects. The choice between inclusion and exclusion of a mediator in the research model is a matter of conciseness versus richness – including the mediator

can facilitate a concise explanation of the dependent variable, whereas excluding the mediator can provide a rich understanding of individual antecedents. Such choices are certainly not alien to the IS discipline. For example, in the long-lasting technology acceptance research stream, some studies follow the original TAM to investigate the indirect effects of perceived usefulness (PU) and ease of use (PEOU) on behavioral intention that are mediated by attitude, while others exclude attitude and examine the direct effects of PU and PEOU (Venkatesh et al., 2003). In addition, our research model posits that avoidance motivation is influenced by an interaction between perceived threat and safeguard effectiveness.
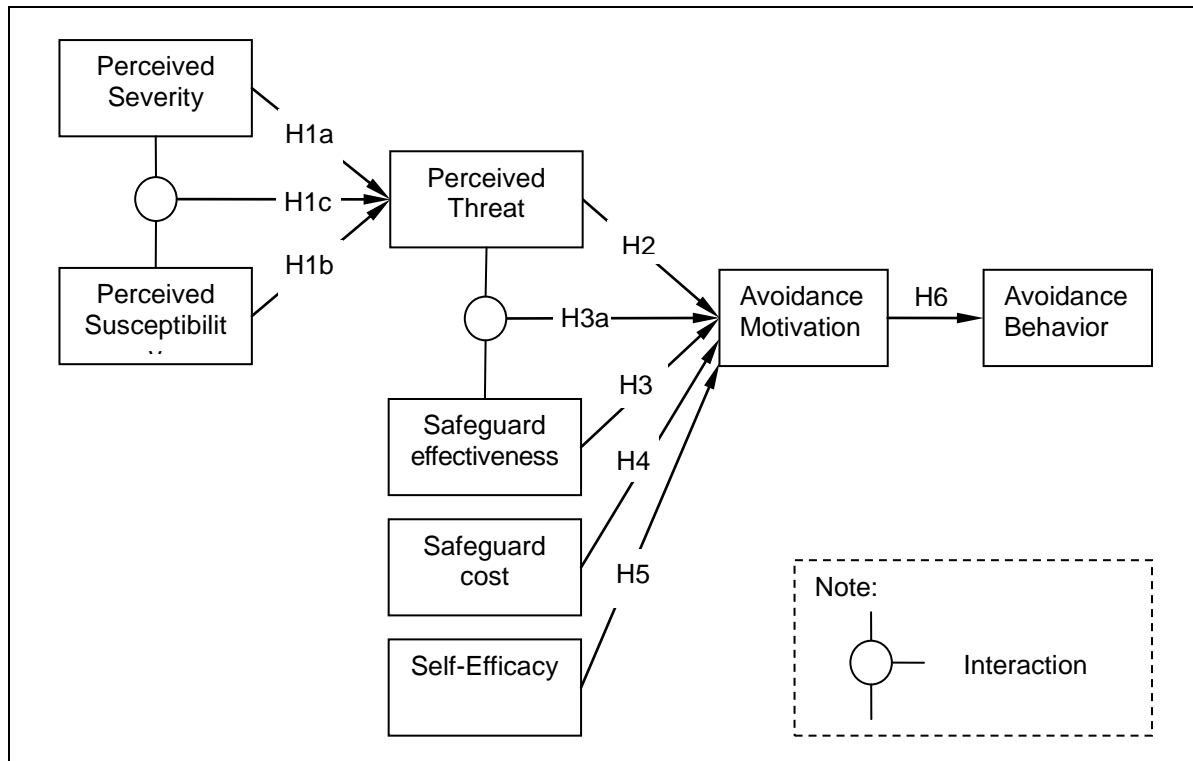
Figure 1. Research model

Perceived threat is defined as the extent to which an individual perceives the malicious IT as dangerous or harmful. IT users develop a perception of threat by monitoring their computing environment and detecting potential dangers. Based on health psychology (Janz and Becker, 1984; Rogers, 1983; Weinstein, 2000) and risk analysis (Baskerville, 1991a), we propose that the threat perception is shaped by two antecedents: perceived susceptibility and perceived severity. Perceived susceptibility is defined as an individual's subjective probability that a malicious IT will negatively affect him or her, and perceived severity is defined as the extent to which an individual perceives that negative consequences caused by a malicious IT will be severe (Liang and Xue, 2009). Health psychology research strongly supports the effect of the susceptibility and severity perceptions on the threat perception. Prior studies on health protective behavior have provided theoretical and empirical evidence that health threats are defined by the perceived probability that harm will occur if no action is taken and the perceived severity of the harm (Weinstein, 2000). Specifically, the health belief model (Janz and Becker, 1984; Rosenstock, 1974) posits that perceived probability and severity of negative consequences give rise to the health threat perception, which motivates individuals to take protective actions. IT security research has studied perceived susceptibility and severity with inconsistent results. Woon et al. (2005) find that perceived vulnerability (susceptibility) does not predict whether individuals will enable their home wireless network security, but perceived severity does. Ng et al. (2009) show that perceived susceptibility affects users' email security behavior, but perceived severity does not. Workman et al. (2008) reveal that perceived vulnerability and severity both have an effect on user IT security behavior. Despite conflicting findings, the consensus among researchers is that IT users evaluate the susceptibility and severity of negative consequences to determine the security

threat they are facing. Therefore, we propose that both perceived susceptibility and severity contribute to the threat perception.

> *H1a: Perceived susceptibility of being attacked by malicious IT positively affects perceived threat.*
> *H1b: Perceived severity of being attacked by malicious IT positively affects perceived threat.*

We contend that perceived susceptibility and severity have an interaction effect when shaping the threat perception. The conceptual connotation of threat is similar to risk, which is calculated in risk analysis research by multiplying the probability and cost of potential damage (Baskerville, 1991a; Baskerville, 1991b; Baskerville, 1993). The multiplication of two variables essentially represents an interaction. The interaction between susceptibility and severity perceptions suggests that the relationship between either of them and perceived threat will disappear if the other variable is scored zero. For example, Kansas residents do not think of hurricanes as a threat to them because they believe it is almost impossible for a hurricane to make landfall in Kansas, although they are fully aware of their destructive wind power. Similarly, when individuals perceive that a malicious IT has no chance of bothering them, they are unlikely to feel threatened, even if the malicious IT can cause serious damages. They will also not feel threatened when they believe that the harmful outcome of a malicious IT is not at all severe, no matter how likely it is to occur.

The interaction between perceived severity and susceptibility is basically a moderation phenomenon. That is, perceived susceptibility positively moderates the relationship between perceived severity and threat, or vice versa. The relationship between perceived severity and the threat can be seen as a function of perceived susceptibility, so that the higher the perceived susceptibility, the stronger the severity-threat relationship. For example, online gamers may face two viruses: one rarely affects online game software (low susceptibility) and the other is spread widely on game websites (high susceptibility). As the severity perception of both viruses increases, the threat perception of the second virus will increase more rapidly than that of the first. Mathematically speaking, the linear regression line between perceived threat and severity for the second virus will be steeper, or have a greater slope, than that of the first virus. This is because when the perceived susceptibility of a malicious IT is high, users are more sensitive to changes in its severity level. The same logic applies to the role of perceived severity in moderating the susceptibility-threat relationship.

> *H1c: Perceived susceptibility and perceived severity have a positive interaction effect on perceived threat.*

Maslow's hierarchy of needs suggests that the safety of one's resources and property is a basic human need (Maslow, 1943). The hedonic principle asserts that people tend to approach pleasure and avoid pain (Freud, 1915; James, 1890). IT threats can cause painful privacy and financial losses. Thus, when users perceive an IT threat, they are motivated to avoid it. Avoidance motivation is defined as the degree to which IT users are motivated to avoid IT threats by taking safeguarding measures. As the threat perception intensifies, individuals are more motivated to get away from the danger. This positive relationship has been confirmed by numerous studies on health protective behavior (Rippetoe and Rogers, 1987; Rosenstock, 1974; Tanner et al., 1991; Weinstein, 1993). As Liang and Xue (2009) articulate, malicious IT and diseases are similar because both are rogue agents that invade a system to cause malevolent changes. Therefore, people's responses to health threats tend to be similar to their responses to IT threats. Based on the empirical evidence from health psychology, we propose that perceived threat of malicious IT positively affects avoidance motivation.

> *H2: Perceived threat positively affects avoidance motivation.*

After a threat is perceived, users start the coping appraisal process to evaluate potential safeguarding measures. Based on prior research (Bandura, 1982; Compeau and Higgins, 1995; Maddus and Rogers, 1983; Weinstein, 1993), we suggest that people assess a safeguarding measure by considering how it effectively counters the IT threat, what costs are associated with it, and how confident they feel about using it. Hence, users appraise three constructs: safeguard effectiveness, safeguard cost, and self-efficacy. Taking all three constructs into consideration, users will be able to assess how avoidable the IT threat is if the safeguard is employed. The more likely a safeguard makes the threat of malicious IT avoidable, the more motivated users are to adopt it.

Safeguard effectiveness is defined as the subjective assessment of a safeguarding measure regarding how effectively it can be applied to avoid the IT threat. It reflects the user perception of the objective outcomes produced by using the safeguard, which is akin to the notion of outcome expectancy (Bandura, 1982). It is also similar to the concept of perceived benefits in the health belief model (Janz and Becker, 1984, Rosenstock, 1974) and the concept of response efficacy in protection motivation theory (Rogers, 1975; Rogers, 1983), both of which have been found to predict behavior likelihood or motivation. Previous studies on IT security have consistently suggested that safeguard effectiveness can motivate users to perform security behaviors (Anderson and Agarwal, 2006; Ng et al., 2009; Woon et al., 2005).

> *H3: Safeguard effectiveness positively affects avoidance motivation.*

Perceived threat and safeguard effectiveness can possibly interact with each other to influence avoidance motivation. Their interaction can be viewed from two perspectives. First, perceived threat can be viewed to negatively moderate the relationship between safeguard effectiveness and avoidance motivation. According to TTAT, when the threat level is high, users tend to experience emotional disturbance caused by the perilous prospect of the threat (Liang and Xue, 2009). Users not only perform problem-focused coping to counter the objective threat, but also utilize emotion-focused coping to mitigate their emotional uneasiness. This proposition of TTAT is consistent with health psychology research, which finds that individuals under health threats are likely to experience psychological stress and use various emotion-focused coping strategies to maintain their psychological well-being (Carver and Scheier, 1982; Lazarus, 1966). While emotion-focused coping helps users maintain an emotional balance, it also reduces their alertness to the threat as well as their reliance on safeguarding measures to cope with the threat. As a result, the impact of the safeguarding measure on avoidance motivation diminishes. For example, an often used emotion-focused coping mechanism is to escape from the situation by trying not to think about it. Although the user knows that the threat is present, she blocks it from her rational thinking. As a result, the relationships between safeguard effectiveness and avoidance motivation at high threat levels become weaker than those at low threat levels.

Second, safeguard effectiveness can be viewed to negatively moderate the relationship between perceived threat and avoidance motivation. Safeguard effectiveness reflects how much control users have over the threat by using a safeguard. Whereas coping theory predicts that people are likely to perform problem-focused coping when they feel in control of the situation (Beaudry and Pinsonneault, 2005; Lazarus and Folkman, 1984), the confidence that things are under one's control is likely to make the person complacent about the situation. Similarly, knowing that the safeguarding measure can effectively reduce the threat, a computer user will not be so eager to cope with it, although she is fully aware of the threat's presence. As a result, as the level of safeguard effectiveness increases, users tend to feel less motivated to avoid the threat.

> *H3a: Perceived threat and safeguard effectiveness have a negative interaction effect on avoidance motivation.*

Safeguard cost refers to the physical and cognitive efforts — such as time, money, inconvenience and comprehension — needed to use the safeguarding measure (Liang and Xue, 2009). These efforts tend to create barriers to behavior and reduce behavioral motivation, because individuals often perform a cost-benefit analysis before they decide to take an action. For example, people usually compare the benefits and costs of a certain health behavior before they decide to engage in it, and they are unlikely to adopt the behavior if the cost is too high (Janz and Becker, 1984; Rosenstock, 1974). Prior IT security research also finds that costs associated with network security significantly reduces the likelihood that individuals enable their home wireless network security (Woon et al., 2005). Hence, user motivation to avoid the IT threat is expected to be dampened by the potential cost of using the safeguard.

> *H4: Safeguard cost negatively affects avoidance motivation.*

In addition, self-efficacy, defined as users' confidence in taking the safeguarding measure, is an important determinant of avoidance motivation. The inclusion of self-efficacy in TTAT is consistent with Bandura's (1982) argument that "in any given instance, behavior would be best predicted by considering both self-efficacy and outcome beliefs" (p. 140). Self-efficacy has been examined by

numerous studies and its relationship with IT adoption intent is well established (Agarwal et al., 2000; Bandura, 1977; Bandura, 1982; Chau, 2001; Compeau et al., 1999; Venkatesh, 2000). In the IT security context, the safeguarding measure is often an IT behavior (e.g., installing anti-virus software, turning off cookies, editing the computer registry file, etc.). Prior research has demonstrated that users are more motivated to perform IT security behaviors as the level of their self-efficacy increases (Ng et al., 2009; Woon et al., 2005; Workman et al., 2008). Therefore, the higher the users' self-efficacy for the safeguarding measure, the stronger their motivation to avoid IT threats by using the measure.

H5: Self-efficacy positively affects avoidance motivation.

In this research, we do not differentiate between motivation and intention. Essentially, avoidance motivation can be represented by the behavioral intention to use the safeguard. As asserted by cognitive theorists (Ajzen, 1991; Ajzen and Fishbein, 1980; Fishbein and Ajzen, 1975), behavioral intention is a strong predictor of actual behavior. This relationship has been confirmed by a large number of IT adoption studies (e.g., Venkatesh et al., 2003). Consistent with prior research, we argue that users with a stronger avoidance motivation are more likely to engage in the avoidance behavior of using the safeguard.

H6: Avoidance motivation positively affects the avoidance behavior of using the safeguard.

4. Methodology

4.1. Data Collection

We conducted a survey study to test the model. We selected spyware and anti-spyware software as the malicious IT and safeguarding measure, respectively. Spyware is a relatively new threat, and many people still have limited knowledge about it. We expected the newness of spyware to result in a wide range of variance in the constructs of our research model, which facilitates the detection of moderation effects. We created an online questionnaire that included two sections. The first section contained items for perceived susceptibility, severity, and threat, safeguard effectiveness, safeguard cost, and self-efficacy. The second section contained items for avoidance motivation and avoidance behavior. We administered the online questionnaire to 166 business students at a major U.S. university. Respondents were asked to complete the first section at the beginning of a class and complete the second section at the end of the class. Extra course credits were given as an incentive. A total of 152 students completed the survey providing a a response rate of 91.56 percent. The average age of the respondents was 23 (SD = 3.99) and most of them were male (66.3 percent). They had advantage of 8.22 years of Internet experience (SD = 2.46).

4.2. Measurement Development

We developed most the measurements based on their theoretical meaning and relevant literature. Perceived threat was measured by items created on the basis of its substantive meaning (Rosenstock, 1974). The items assessed respondents' perception of the potential harm, danger, or peril that spyware imposes. We developed the scales for perceived susceptibility based on health behavior research (Saleeby, 2000); they evaluate the likelihood and possibility of spyware's occurrence.

TTAT posits that IT users' computer-related well-being includes two dimensions: information privacy and computer performance and malicious IT could damage both dimensions (Liang and Xue, 2009). Therefore, users' severity perceptions should relate to the two dimensions. To develop the measurement for perceived severity, we referred to the privacy literature in IS (Smith et al., 1996) and practitioner journals that report the negative impacts of spyware (Schultz, 2003; Shaw, 2003; Sipior et al., 2005; Stafford and Urbaczewski, 2004). The items taped into users' concerns about both loss of personal information and degraded computer performance related to processing speed, Internet connection, and software applications.

We developed the items of safeguard effectiveness based on relevant health behavior research (Champion and Scott, 1997; Saleeby, 2000). We derived the items for safeguard cost from Milne et al. (2002) and Saleeby (2000). We measured self-efficacy with the items developed by Compeau and

Higgins (1995), making minor modifications to adapt it to the anti-spyware context. The measures for avoidance motivation were based on the behavioral intention measures from technology adoption research (Davis, 1989; Davis et al., 1989), with a focus on threat avoidance rather than IT adoption. We measured IT threat avoidance behavior with two self-developed items.

We evaluated the perceived severity items using by a seven-point scale anchored at 1="Innocuous" and 7="Extremely devastating." The self-efficacy items were assessed by a 10-point scale anchored at 1="Not at all confident" and 10="Totally confident." All the other items were evaluated by a seven-point scale anchored at 1="Strongly disagree" and 7="Strongly agree."

We showed the initial pool of items to 20 regular personal computer users to elicit feedback therough face-to-face interviews. Based on the feedback, we slightly revised the wording of some measurement items. As shown in Appendix 1, the final questionnaire contained five items for perceived threat, 10 items for perceived severity, five items for perceived susceptibility, six items for safeguard effectiveness, three items for safeguard cost, 10 items for self-efficacy, three items for avoidance motivation, and two items for avoidance behavior (see Appendix 1).

5. Data Analysis and Results

We used Partial Least Squares (PLS), specifically SmartPLS 2.0 (Ringle et al., 2005), for validating the measurements and testing the hypotheses. PLS employs a component-based approach for model estimation, and it is not highly demanding on sample size and residual distributions (Gefen et al., 2000). PLS is best suited for testing complex structural models because it avoids inadmissible solutions and factor indeterminacy (Fornell and Bookstein, 1982).

5.1. Measurement Validation

We assessed convergent and discriminant validity of the measurements by two criteria: (1) each item should have a higher loading on its hypothesized construct than on other constructs , and (2) the square root of each construct's Average Variance Extracted (AVE) should be greater than its correlations with other constructs (Fornell and Larcker, 1981). First, following Gefen et al. (2000), we conducted a PLS confirmatory analysis. The results show that items have much higher self-loadings than cross-loadings (Appendix 2). Second, we computed each construct's AVE and the AVE's square root is greater than the construct's cross correlations with other constructs (Table 1). In addition, we calculated each construct's composite reliability coefficient. As Table 1 shows, all coefficients are over .90, much greater than the recommended value of .70 (Nunnally, 1978), suggesting adequate measurement reliability.

Table 1. Correlation matrix and AVEs for constructs										
Constructs	**R**	**AVE**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1. Perceived Susceptibility	.972	.875	.935							
2. Perceived Severity	.945	.635	.292	.797						
3. Perceived Threat	.936	.746	.397	.496	.864					
4. Safeguard Effectiveness	.981	.894	.313	.210	.410	.946				
5. Safeguard Cost	.890	.730	-.239	-.134	-.218	-.570	.854			
6. Self-efficacy	.957	.692	.199	.197	.245	.406	-.385	.832		
7. Avoidance Motivation	.977	.934	.314	.308	.509	.644	-.483	.454	.966	
8. Avoidance Behavior	.920	.852	.195	.380	.181	.406	-.258	.283	.444	.923

Note: The diagonal elements represent square roots of AVE.

Although we attempted to mitigate the concern of common method variance (CMV) by measuring exogenous and endogenous variables in two sections of the online survey, we still measured all of the constructs by respondents' self-report, which might introduce common method bias into our data analysis. We assessed CMV with two tests. First, we performed Harman's one-factor test by conducting an exploratory factor analysis and inspecting the unrotated factor solution (Podsakoff et al., 2003; Podsakoff and Organ, 1986). Large common method variance is present when a single

factor emerges or one general factor accounts for most of the covariance among the measures. Eight factors emerged, which explained 80.83 percent of the data variance, and the largest variance explained by a factor was only 17.56 percent, suggesting that CMV is not a serious concern.

Second, following Podsakoff et al. (2003) and Liang et al. (2007), we used structural equation modeling (SEM) to examine the influence of CMV. Using AMOS, we estimated a confirmatory factor model that included the eight principal constructs. Then we added into this model a common method factor that took all of the eight constructs' indicators as its own indicators. In this approach, the variance of a specific observed indicator is partitioned into three components: trait, method, and random error. If the data was influenced by CMV, the second model would fit the data significantly better than the first. We compared the two model's Chi square and found the difference to be not significant, suggesting that the structural relationships among constructs are unlikely to be biased by CMV (Williams et al., 2003).

5.2. Model Testing

Figure 2 shows the model testing results. Our model accounts for 33 percent of variance in perceived threat, 56 percent of variance in avoidance motivation, and 21 percent of variance in avoidance behavior. As hypothesized, perceived threat is significantly determined by perceived severity (b = .27, p < .01) and perceived susceptibility (b = .41, p < .01), providing support for H1a and H1b. To examine whether perceived threat mediates the effects of perceived susceptibility and perceived severity on avoidance motivation, we tested two competing PLS models. First, we tested a model that linked perceived severity and susceptibility to avoidance motivation. The PLS result showed that both links are significant. Second, we added perceived threat to the previous model and added three links: from severity to threat, from susceptibility to threat, and from threat to avoidance motivation. The PLS result of testing this model showed that the two links from severity and susceptibility to avoidance motivation were non-significant, the two links from severity and susceptibility to threat were significant, and the link from threat to avoidance motivation was significant. According to Baron and Kenny (1986), these results show that the influences of susceptibility and severity on avoidance motivation are fully mediated by perceived threat.
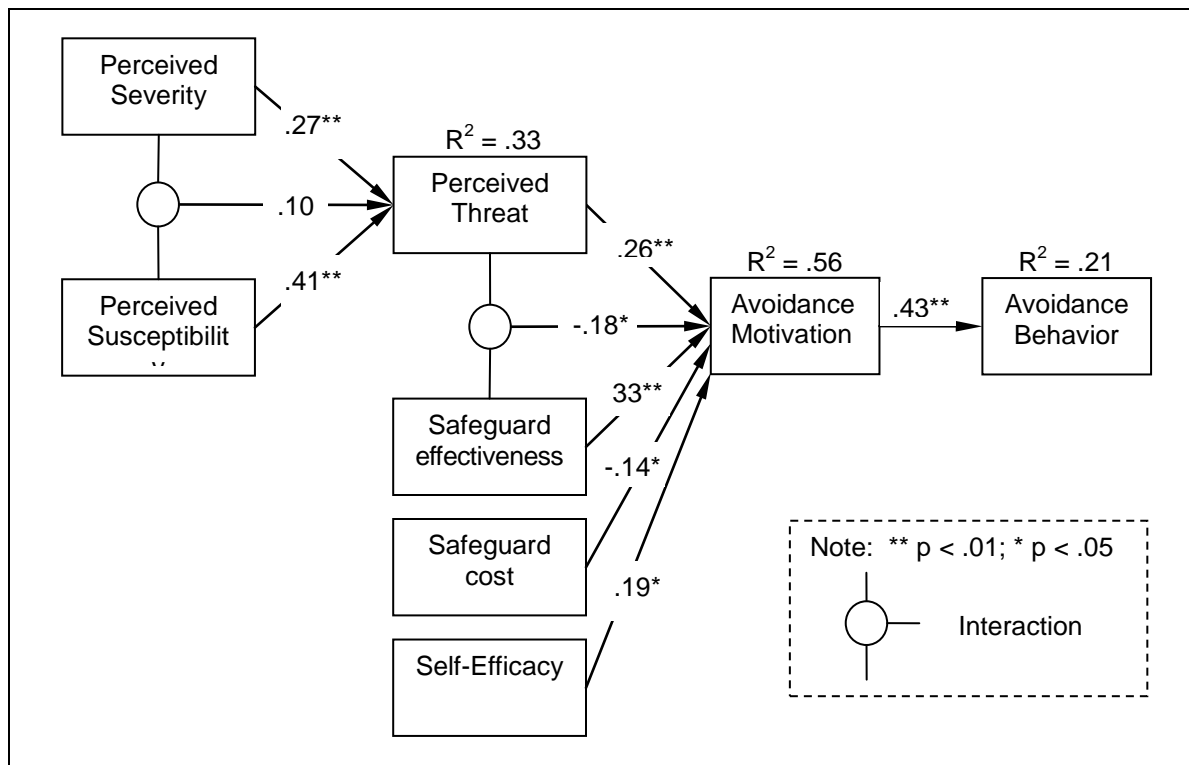
Figure 2. Model testing results

As Figure 2 shows, avoidance motivation is significantly determined by perceived threat (b = .26, p < .01), safeguard effectiveness (b = .33, p < .01), safeguard cost (b = -.14, p < .05), and self-efficacy (b = .19, p < .05). These findings lend support to H2, H3, H4, and H5. Finally, avoidance motivation is found to significantly influence avoidance behavior (b = .43, p < .01), supporting H4.

To evaluate the interaction effects proposed by H1c and H3a, we followed a product-indicator approach (Chin et al., 2003). We created the interaction variables by cross-multiplying the items of perceived susceptibility and severity, and perceived threat and safeguard effectiveness. All of the items were standardized before multiplication to reduce multicollinearity (Aiken and West, 1991). As Figure 2 shows, the interaction between perceived severity and susceptibility is not significant (b = .10, p > .05), while the interaction between perceived threat and safeguard effectiveness is (b = .18, p < .05). The results do not support H1c. To further validate the interaction between threat and safeguard effectiveness, we calculated the effect size (f^2) by comparing the R^2 value between the main and the interaction effect (Chin et al., 2003).[1] The effect size of the interaction is .05, which denotes a small to medium effects (Cohen, 1988). Therefore, we find strong evidence to support H3a, which suggests that if the standardized value of perceived threat is increased by 1, the regression coefficient between safeguard effectiveness and avoidance motivation will decrease by 0.18, or vice versa.

In summary, our data analysis results provide support to all of the hypotheses except H1c. In the PLS model, we included age, gender, and Internet experience as control variables on avoidance motivation and avoidance behavior. None of these control variables was found to have a significant effect on either dependent variable.

6. Discussion

This study empirically investigated why personal computer users we anti-spyware to avoid the threat of spyware. We paid particular attention to perceived threat because it plays a pivotal role in influencing users' avoidance behavior. We validate a research model derived from TTAT (Liang and Xue, 2009) using survey data. Data analysis results reveal that the model is able to explain a large amount of variance in users' motivation to avoid IT threats (56 percent) and actual avoidance behavior (21 percent). This paper conveys a simple, yet powerful message – to motivate computer users to avoid IT threats, they need to be convinced that the threats exist and are avoidable. If users fail to see a threat, they will not act to avoid it. If they see the threat but believe it is unavoidable, they will not act to avoid it, either. Thus, both the threat appraisal and the coping appraisal are necessary to motivate security behaviors. Furthermore, we demonstrate that to develop a threat perception, users need to be aware of the likelihood and severity of being attacked by the IT threat. Users evaluate a safeguarding measure from three aspects, taking into account safeguard effectiveness, cost, and their confidence in using the safeguard. We also find that perceived threat and safeguard effectiveness have a negative interaction, suggesting that when the level of either construct is high, the other construct's relationship with avoidance motivation will be weakened. This interesting finding could generate new insights in IT users' threat avoidance behavior.

The only hypothesis not supported is H1c, which proposes the interaction between perceived severity and susceptibility. Based on Aguinis (1995), we contend that a lack of power might have impeded detection of the interaction. There are three plausible explanations. First, the variance in perceived susceptibility and severity has a range restriction, because our sample is not a random sample and cannot represent the entire personal computer user population (Aguinis, 1995). Second, the "scale coarseness" of avoidance motivation might have reduced the statistical power (Bobko and Russell, 1994). Whereas the interaction variable has a possible range of 7 x 7 = 49 distinct responses, avoidance motivation only has a "coarse" 7-point Likert scale. Therefore, information regarding the relationship between avoidance motivation and the interaction variable is lost, and power is reduced. Finally, a large sample size is needed to detect a small moderation effect (Carte and Russell, 2003). Using G*Power, we estimated the sample size required to achieve the power of 0.8 for a small effect size (f^2 = 0.02) in multiple regression and found the required sample size is 395. If the effect size of

---

[1] f^2 = [R^2(interaction model) − R^2(main effect model)] / [1 - R^2(interaction model)]

the susceptibility-severity interaction is small, our sample size will not provide enough power to detect it.

6.1.   Implications for Research

Numerous forms of malicious IT continuously jeopardize the security of contemporary computing environments. Yet theory-based empirical research that explains computer users'' voluntary IT threat avoidance behavior is lacking. Most existing security research on individual behavior is focused on organizational settings where the threat avoidance behavior is mandatory (e.g., D'Arcy et al., 2009; Straub and Welke, 1998). These studies often draw on general deterrence theory to model IT users as passive subjects who comply with IT security policies because noncompliance would be disciplined. While this approach makes sense in mandatory settings, it cannot be applied to IT users outside the organizational context who perform security behaviors volitionally. Although a few studies have examined individual users' security behavior, the findings are largely inconsistent and sometimes contradictory (e.g., Ng et al., 2009; Woon et al., 2005; Workman et al., 2008). This research fills the gap in the literature. Drawing on TTAT (Liang and Xue, 2009), we offer an enhanced understanding of IT users' voluntary technology threat avoidance behavior. TTAT highlights dual cognitive processes: threat appraisal and coping appraisal. First, users appraise the threat coming from malicious IT for susceptibility and severity. Second, users appraise the safeguard's effectiveness in reducing the threat and their own self-efficacy in using the safeguard. Computer users are likely to employ the safeguard if there is a threat, the threat can be averted by the safeguard, and they have sufficient confidence in using the safeguard. Perceived threat is essential in this context, since it triggers the entire coping process. However, little behavioral research in the IT security area theorizes threat as a formal construct. This study explicitly examines threat and its impact on avoidance motivation, shedding light on IT threat avoidance behavior in voluntary settings.

We empirically demonstrate that perceived threat is determined by both perceived susceptibility and severity. While this notion has long been accepted by health psychology and risk analysis researchers, it is rarely seen in behavioral research on IT security. Our findings suggest that both constructs are necessary antecedents of perceived threat. As Table 1 shows, these two constructs are weakly correlated (r = .29), suggesting they are largely independent of each other. Thus, ignoring either one might lead to a biased estimation of perceived threat.

The negative interaction between perceived threat and safeguard effectiveness is particularly provocative. First, it is counterintuitive. Intuitively, one would expect a positive interaction, i.e., at a higher threat level, the relationship between safeguard effectiveness and avoidance motivation is stronger, or vice versa. To explain this counterintuitiveness, TTAT posits that high threat causes emotion-focused coping, which reduces individuals' sensitivity to safeguard effectiveness. An alternative explanation is that when the safeguard is highly effective, users' motivation to avoid the threat is lowered because they feel that they can use the safeguard to take control of the situation. Both explanations seem plausible. Further research on refined cognitive processes under threat is needed to find out which explanation is closer to the truth.

In summary, this paper generates initial empirical evidence supporting TTAT. Although TTAT provides a theoretically convincing account of individual IT security behavior, it has not been empirically validated. Given that TTAT is fairly complicated, involving a process model, a variance model, and a number of constructs, this research can only offer partial validation. Much more research is needed to test the various propositions of TTAT and shed light on the security behaviors of individual IT users.

6.2.   Implications for Practice

This study examines user IT threat avoidance in the context of personal computer usage, because most users are particularly vulnerable to security breaches. Whereas organizations can and do implement security governance programs to regulate employees' threat avoidance behavior (Gordon et al., 2006), users at home in a non-work settings are free agents acting on their own and are easy prey to IT threats. In addition, organizations may have a centralized or decentralized IT security environment (Warkentin and Johnston, 2006). In the centralized IT security environment, security is managed at the enterprise level, and employees have no choice to opt out. In contrast, in the

decentralized IT security environment, employees engage in voluntary protective actions such as enabling their personal firewall and updating their own antivirus and/or antispyware software. These employees, like home computer users, are highly likely to engage in unsafe computer behaviors and become weak links in the organizational security system. Security education, awareness, and training are much needed to help these users cope with IT threats. Academic research that takes a cognitive behavioral perspective to examine how users deal with IT threats can contribute to the effectiveness of such IT security programs.

This study can inform IT security programs in several aspects. First, it endorses the value of security education, awareness, and training programs. Individuals will be more motivated to avoid IT threats and use safeguarding measures if these programs help them develop threat perceptions, realize the effectiveness of safeguarding measures, lower safeguard costs, and increase self-efficacy. Second, this study suggests that security awareness programs should emphasize both the likelihood of IT threats and the severity of losses caused by the threats. Third, the negative interaction between perceived threat and safeguard effectiveness suggests that the relationship between safeguard effectiveness and avoidance motivation is lower when the threat level is high than when it is low. This implies that overly high threat perceptions could be "too much of a good thing." It is probably ill-advised to emphasize excessively how universal and how disastrous IT threats are. TTAT suggests that emotion-focused coping is a possible culprit that confuses users' motivation systems at high threat levels. Public security education should draw attention to possible emotion-focused coping and help people understand how they unintentionally engage in emotion-focused coping and how to stop. Such information would help people focus on problem-focused coping, thus reducing the negative effects of high threat perceptions.

6.3.   Limitations and Future Research

This study has several limitations. First, we used college students as a convenience sample. College students do not represent the population of general personal computer users. They are younger, more IT-savvy, and probably more knowledgeable about malicious IT than average home users. Hence, researchers should be cautious when generalizing our findings to other personal computer users. Given that this research is more focused on understanding how the constructs work in the model to explain IT security behavior than on generalizability, it is justifiable to use a subset of the computer user population as our sample. In addition, it is practically infeasible to obtain a random sample of the entire population of personal computer users that we can claim to be truly representative and free from the concern of generalizability. Future research is needed to confirm our findings using different samples.

Second, for the purpose of empirical testing, we selected spyware as the malicious IT and anti-spyware software as the safeguarding measure. This does not necessarily mean that the source of an IT threat or the safeguarding measure must be an IT. The source of a threat could be a person (e.g., a hacker) or an event (e.g., denial of service) and the safeguarding measure could be a behavior (e.g., updating a password) or an inaction (e.g., stop downloading freebies). Research can be conducted with different threat sources and safeguards to examine whether the findings of this study will change.

Third, to fully understand the negative interaction between perceived threat and safeguard effectiveness, emotion-focused coping should be empirically measured and examined. It is interesting to study what conditions give rise to emotion-focused coping and how it interacts with perceived threat and safeguard effectiveness to influence avoidance behavior.

Fourth, we did not include perceived avoidability in this research, although TTAT suggests that it mediates the effects of safeguard effectiveness, safeguard cost, and self-efficacy on avoidance motivation. While it is found that all of these three constructs significantly influence avoidance motivation, we have no empirical evidence regarding whether perceived avoidability can mediate users' appraisal of all aspects of the safeguarding measure. Future research should develop an appropriate measure for perceived avoidability and appropriately examine its mediating role.

In summary, this research provides preliminary validation for a simplified variance model of TTAT,

suggesting that TTAT is powerful in explaining individual users' IT security behavior. Due to limitations, this research does not validate TTAT in its entirety. Some theoretical nuances related to emotion-focused coping and perceived avoidability should be illustrated with empirical evidence in future research.

7. Conclusions

This study investigates personal computer users' IT threat avoidance behaviors. We derive a research model TTAT and test it using survey data collected from 152 personal computer users. Data analyses reveal several major findings. First, perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy influence avoidance motivation, which determines avoidance behavior. Second, perceived threat is determined by perceived susceptibility and severity and fully mediates their effects. Finally, perceived threat negatively moderates the relationship between safeguard effectiveness and avoidance motivation. These findings provide an enriched understanding of users' IT threat avoidance behavior in the personal computer usage context where security behavior is voluntary. More research is called for to test TTAT more comprehensively and in other settings.

Acknowledgements

References

Agarwal, R., V. Sambamurthy, and R. M. Stair (2000) "Research Report: The Evolving Relationship Between General and Specific Computer Self-Efficacy - An Empirical Assessment," *Information Systems Research* (11) 4, pp. 418-430.

Aguinis, H. (1995) "Statistical power problems with moderated multiple regression in management research," *Journal of Management* (21) 6, pp. 1141-1158.

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

Ajzen, I. (1991) "The theory of planned behavior," *Organizational Behavior & Decision Processes* (50), pp. 179-211.

Ajzen, I. and M. Fishbein (1980) *Understanding attitudes and predicting behavior*. Englewood Cliffs, NJ: Prentice Hall.

Anderson, C. L. and R. Agarwal (2006) Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions, in *International Conference on Information Systems*, pp. 1543-1561. Milwaukee, WI.

Aytes, K. and C. Terry (2004) "Computer security and risky computing practices: A rational choice perspective," *Journal of Organizational and End User Computing* (16) 3, pp. 22-40.

Bagchi, K. and G. Udo (2003) "An analysis of the growth of computer and internet security breaches," *Communications of the AIS* (12), pp. 684-700.

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

Bandura, A. (1982) "Self-efficacy mechanism in human agency," *American Psychologist*) 37, pp. 122-147.

Baron, R. and D. Kenny (1986) "The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations," *J Person Soc Psych* (51) 6, pp. 1173-1182.

Baskerville, R. (1991a) "Risk analysis as a source of professional knowledge," *Computer & Security* (10) 8, pp. 749-764.

Baskerville, R. (1991b) "Risk analysis: an interpretive feasibility tool in justifying information systems security," *European Journal of Information Systems* (1) 2, pp. 121-130.

Baskerville, R. (1993) "Information systems security design methods: implications for information systems development," *ACM Computing Surveys* (25) 4, pp. 375-414.

Beaudry, A. and A. Pinsonneault (2005) "Understanding user responses to information technology: A coping model of user adaptation," *MIS Quarterly* (29) 3, pp. 493-524.

Bobko, P. and C. J. Russell (1994) "On theory, statistics, and the search for interactions in the organizational sciences," *Journal of Management* (20), pp. 193-200.

Carte, T. and C. Russell (2003) "In Pursuit of Moderation: Nine Common Errors and Their Solutions," *MIS Quarterly* (27) 3, pp. 479-501.

Carver, C. S. and M. F. Scheier (1982) "Control theory: A useful conceptual framework for personality-social, clinical, and health psychology," *Psychological Bulletin* (92) 1, pp. 111-135.

Champion, V. and C. Scott (1997) "Reliability and validity of breast cancer screening belief scales in African American women," *Nursing Research* (46) 6, pp. 331-337.

Chau, P. Y. K. (2001) "Influence of computer attitude and self-efficacy on IT usage behavior," *Journal of End User Computing* (13) 1, pp. 26.

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

Cohen, J. (1988) *Statistical Power Analysis for the Behavioral Sciences*, 2nd edition. Hillsdale, NJ: Lawrence Erlbaum.

Compeau, D. R. and C. A. Higgins (1995) "Computer self-efficacy: development of a measue and initial test," *MIS Quarterly* (19), pp. 189-211.

Compeau, D. R., C. A. Higgins, and S. Huff (1999) "Social cognitive theory and individual reactions to computing technology: a longitudinal study," *MIS Quarterly* (23) 2, pp. 145-158.

Consumer Reports. (2009) *State of the Net 2009*. Consumer Reports National Research Center.

CSI. (2009) *Computer crime & security survey 2009*. Computer Security Institute.

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

Davis, F. D. (1989) "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13) 3, pp. 319-338.

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

Day, J. C., A. Janus, and J. Davis. (2005) *Computer and Internet Use in the United States: 2003*. US Census Bureau.

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

Edwards, J. (1992) "A cybernetic theory of stress, coping, and well-being in organizations," *Academy of Management Review* (17) 2, pp. 238-274.

Fishbein, M. and I. Ajzen (1975) *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Fornell, C. and F. L. Bookstein (1982) "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory," *Journal of Marketing Research* (19pp. 440-452.

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

Freud, S. (1915) Repression, in, vol. XIV*Complete psychological works of Sigmund Freud*, London: Hogarth.

Gefen, D., D. Straub, and M. Boudreau (2000) "Structural equation modeling and regression: guidelines for research practice," *Communications of the AIS* (4) 7.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and R. Richardson. (2006) *2006 CSI/FBI computer crime and security survey*. Computer Security Institute.

Handy, C. (1995) "Trust and the virtual organization," *Harvard Business Review* (73) 3, pp. 40-50.

James, W. (1890) *The principles of psychology*. Vol. 2. New York: Henry Holt & Co.

Janz, N. K. and M. H. Becker (1984) "The health belief model: a decade later," *Health Education Quarterly* (11) 1, pp. 1-45.

Jones, S. and S. Fox. (2009) *Generations Online in 2009*. Pew Internent & American Life Project.

Lazarus, R. (1966) *Psychological stress and the coping process*. New York: McGraw-Hill.

Lazarus, R. and S. Folkman (1984) *Stress, coping, and adaptation*. New York: Springer-Verlag.

Liang, H., N. Saraf, Q. Hu, and Y. Xue (2007) "Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management," *MIS Quarterly,* 31(1), 59-87.

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

Loch, K. D., H. H. Carr, and M. E. Warkentin (1992) "Threats to information systems: Today's reality, yesterday's understanding," *MIS Quarterly* (16) 2, pp. 173-186.

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

Maslow, A. H. (1943) "A Theory of Human Motivation," *Psychological Review* (50) 4, pp. 370-396.

Milne, S., S. Orbell, and P. Sheeran (2002) "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British Journal of Health Psychology* (7), pp. 163-184.

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

Nunnally, J. (1978) *Psychometric theory*, 2nd edition. New York: McGraw-Hill.

Podsakoff, P. M., S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff (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.

Podsakoff, P. M. and D. W. Organ (1986) "Self-reports in organizational research: problems and prospects," *Journal of Management* (12) 4, pp. 531-544.

Ringle, C. M., S. Wende, and A. Will (2005) SmartPLS, 2.0 (beta) edition. Hamburg, Germany.

Rippetoe, P. A. and R. W. Rogers (1987) "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat," *Journal of Personality and Social Psychology* (52) 3, pp. 596-604.

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 process in fear appeals and attitude change: a revised theory of protection motivation, in J. Cacioppo and R. Petty (Eds.) *Social Psychophysiology: a source book*, New York: Guilford Press, pp. 153-176.

Rosenstock, I. M. (1974) "The health belief model and preventive health behavior," *Health Education Monographs* (2pp. 354-386.

Saleeby, J. R. (2000) "Health beliefs about mental illness: an instrument development study," *American Journal of Health Behavior* (24) 2, pp. 83-95.

Schultz, E. (2003) "Pandora's box: spyware, adware, autoexecution, and NGSCB," *Computer & Security* (22) 5, pp. 366-367.

Shaw, G. (2003) "Spyware & Adware: the Risks facing Businesses," *Network Security* (2003) 9, pp. 12-14.

Sipior, J. C., B. T. Ward, and G. R. Roselli (2005) "The ethical and legal concerns of spyware," *Information Systems Management* (22) 2, pp. 39-49.

Smith, H., S. Milberg, and S. Burke (1996) "Information privacy: measuring individuals' concerns about organizational practices," *MIS Quarterly* (20) 2, pp. 167-196.

Stafford, T. F. and A. Urbaczewski (2004) "Spyware: the ghost in the machine," *Communications of the AIS* 14, pp. 291-306.

Straub, D. and R. Welke (1998) "Coping with systems risk: security planning models for management decision making," *MIS Quarterly* (22) 4, pp. 441-469.

Tanner, J. F., J. B. Hunt, and D. R. Eppright (1991) "The protection motivation model: a normative model of fear appeals," *Journal of Marketing* (55), pp. 36-45.

Venkatesh, V. (2000) "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model," *Information Systems Research* (11) 4, pp. 342-365.

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

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

Weinstein, N. D. (1993) "Testing four competing theories of health-protective behavior," *Health Psychology* (12) 4, pp. 324-333.

Weinstein, N. D. (2000) "Perceived probability, perceived severity, and health-protective behavior," *Health Psychology* (19) 1, pp. 65-74.

Williams, L. J., J. R. Edwards, and R. J. Vandenberg (2003) "Recent advances in causal modeling

methods for organizational and management research," *Journal of Management* (29) 6, pp. 903-936.

Woon, I., G. W. Tan, and R. Low (2005) A Protection Motivation Theory Approach to Home Wireless Security, in *International Conference on Information Systems*, pp. 367-380. Las Vegas, NV.

Workman, M., W. H. Bommer, and D. Straub (2008) "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24) 6, pp. 2799-2816.

Appendix 1. Measurement Items for Principal Constructs

Perceived Susceptibility (1 = strong disagree, 7 = strongly disagree)
It is extremely likely that my computer will be infected by spyware in the future
My chances of getting spyware are great
There is a good possibility that my computer will have spyware
I feel Spyware will infect my computer in the future
It is extremely likely that spyware will infect my computer
Perceived Severity (1 = innocuous, 7 = extremely devastating)
Spyware would steal my personal information from my computer without my knowledge
Spyware would invade my privacy
My personal information collected by spyware could be misused by cyber criminals
Spyware could record my Internet activities and send it to unknown parties
My personal information collected by spyware could be subject to unauthorized secondary use
My personal information collected by spyware could be used to commit crimes against me
Spyware would slow down my Internet connection
Spyware would make my computer run more slowly
Spyware would cause system crash on my computer from time to time
Spyware would affect some of my computer programs and make them difficult to use
Perceived Threat (1 = strong disagree, 7 = strongly disagree)
Spyware poses a threat to me
The trouble caused by spyware threatens me
Spyware is a danger to my computer
It is dreadful if my computer is infected by spyware
It is risky to use my computer if it has spyware
Perceived Safeguard Effectiveness (1 = strong disagree, 7 = strongly disagree)
Anti-spyware software would be useful for detecting and removing spyware
Anti-spyware software would increase my performance in protecting my computer from spyware
Anti-spyware software would enable me to search and remove spyware on my computer faster
Anti-spyware software would enhance my effectiveness in searching and removing spyware on my computer
Anti-spyware software would make it easier to search and remove spyware on my computer
Anti-spyware software would increase my productivity in searching and removing spyware on my computer
Perceived Safeguard Cost (1 = strong disagree, 7 = strongly disagree)
I don't have anti-spyware on my PC because …
… I don't know how to get an anti-spyware software
… Anti-spyware software may cause problems to other programs on my computer
… Installing anti-spyware software is too much trouble.
Self-Efficacy (1 = not at all confident, 10 = totally confident)
I could successfully install and use anti-spyware software if …
… there was no one around to tell me what to do
… I had never used a package like it before
… I had only the software manuals for reference

… I had seen someone else doing it before trying it myself
… I could call someone for help if I got stuck
… someone else helped me get started
… I had a lot of time to complete the job
… I had just the built-in help facility for assistance
… someone showed me how to do it first
… I had used similar packages like this one before to do the job
Avoidance Motivation (1 = strong disagree, 7 = strongly disagree)
I intend to use anti-spyware software to avoid spyware
I predict I would use anti-spyware software to avoid spyware
I plan to use anti-spyware software to avoid spyware
Avoidance Behavior (1 = strong disagree, 7 = strongly disagree)
I run anti-spyware software regularly to remove spyware from my computer.
I update my anti-spyware software regularly.

Appendix 2. Cross Loadings of Construct Indicators

Items	Mean	S.D.	SUS	SEV	THR	EFF	COST	SE	AM	AB
SUS1	5.01	1.63	**.92**	.28	.39	.34	-.28	.19	.32	.19
SUS2	4.75	1.67	**.91**	.33	.35	.25	-.19	.14	.30	.20
SUS3	4.94	1.62	**.94**	.24	.32	.25	-.19	.14	.25	.13
SUS4	4.99	1.63	**.95**	.26	.37	.34	-.24	.23	.30	.22
SUS5	4.93	1.60	**.96**	.24	.40	.27	-.22	.21	.28	.17
SEV1	5.03	1.46	.20	**.86**	.48	.12	-.06	.11	.21	.25
SEV2	5.20	1.46	.23	**.84**	.44	.18	-.15	.08	.24	.32
SEV3	5.34	1.54	.16	**.84**	.39	.14	-.09	.14	.15	.29
SEV4	5.21	1.36	.19	**.76**	.28	.10	-.06	.16	.20	.36
SEV5	5.32	1.48	.22	**.84**	.44	.16	-.11	.15	.24	.34
SEV6	5.51	1.53	.25	**.85**	.46	.24	-.11	.19	.26	.27
SEV7	5.44	1.49	.32	**.74**	.33	.25	-.18	.19	.30	.38
SEV8	5.47	1.44	.27	**.70**	.25	.15	-.15	.19	.29	.32
SEV9	5.47	1.48	.22	**.77**	.40	.13	-.04	.14	.30	.29
SEV10	5.49	1.41	.28	**.78**	.37	.16	-.15	.24	.27	.27
THR1	5.55	1.31	.46	.42	**.91**	.44	-.25	.31	.52	.19
THR2	5.38	1.31	.34	.48	**.89**	.30	-.23	.26	.45	.18
THR3	5.53	1.31	.40	.34	**.90**	.34	-.19	.21	.44	.10
THR4	5.36	1.36	.21	.37	**.83**	.37	-.20	.15	.40	.11
THR5	5.24	1.48	.29	.52	**.79**	.30	-.07	.08	.36	.20
EFF1	5.61	1.38	.27	.20	.41	**.95**	-.50	.38	.64	.39
EFF2	5.60	1.31	.28	.19	.41	**.93**	-.49	.32	.60	.39
EFF3	5.60	1.37	.32	.21	.38	**.95**	-.57	.38	.58	.39
EFF4	5.64	1.32	.29	.19	.39	**.95**	-.54	.40	.58	.36
EFF5	5.62	1.27	.33	.19	.38	**.94**	-.55	.41	.59	.38
EFF6	5.62	1.31	.27	.21	.35	**.95**	-.59	.40	.63	.39
COST1	3.05	1.98	-.27	-.09	-.18	-.50	**.87**	-.32	-.44	-.20
COST2	3.33	1.80	-.18	-.03	-.11	-.43	**.79**	-.27	-.34	-.20
COST3	3.02	1.81	-.17	-.21	-.25	-.53	**.90**	-.39	-.45	-.26
SE1	6.82	2.98	.21	.09	.17	.31	-.47	**.75**	.38	.16
SE2	6.65	2.95	.15	.13	.16	.35	-.46	**.78**	.36	.26
SE3	7.08	2.63	.21	.16	.23	.39	-.38	**.86**	.45	.25
SE4	7.45	2.37	.15	.11	.14	.26	-.27	**.87**	.33	.28
SE5	7.83	2.14	.15	.25	.25	.36	-.30	**.88**	.41	.26
SE6	7.87	2.13	.13	.19	.19	.36	-.30	**.83**	.35	.24
SE7	7.63	2.13	.21	.22	.26	.33	-.28	**.85**	.38	.20
SE8	7.29	2.32	.15	.08	.22	.30	-.27	**.83**	.32	.15
SE9	8.09	2.17	.12	.12	.13	.26	-.12	**.78**	.29	.22
SE10	8.06	2.03	.12	.22	.24	.36	-.33	**.86**	.42	.32
AM1	5.43	1.74	.32	.25	.50	.63	-.47	.46	**.97**	.43
AM2	5.54	1.57	.26	.33	.48	.61	-.47	.42	**.96**	.43
AM3	5.49	1.61	.33	.31	.48	.61	-.47	.43	**.97**	.42
AB1	5.71	1.53	.21	.41	.24	.42	-.25	.29	.48	**.95**
AB2	5.19	1.86	.14	.26	.06	.31	-.23	.22	.31	**.89**

Notes: SUS = susceptibility; SEV = severity; THR = threat; EFF = safeguard effectiveness; COST = safeguard cost; SE = self-efficacy; AM = avoidance motivation; AB = avoidance behavior.

About the Authors

Huigang Liang is an assistant professor of management information systems in the College of Business at East Carolina University. His current research interests focus on IT issues at both individual and organizational levels including IT avoidance, adoption, compliance, assimilation, decision process, IT strategy, and healthcare informatics. His research has appeared or will appear in scholarly journals such as MIS Quarterly, Information Systems Research, Journal of the AIS, Drug Discovery Today, Communications of the ACM, Decision Support Systems, and the Journal of Strategic Information Systems. He was ranked 10th worldwide in terms of top-level IS journal publications between 2007 and 2009. He holds a MS in software engineering and a PhD in healthcare information systems from Auburn University.

Yajiong Xue is an assistant professor in the College of Business at East Carolina University. She holds a BS in international pharmaceutical business from China pharmaceutical University, China and a MS in information systems and a PhD in management information technology and innovation from Auburn University. Her research appears in MIS Quarterly, Information Systems Research, Journal of the AIS, Communications of the ACM, Communications of the AIS, Decision Support Systems, IEEE Transactions on Information Technology in Biomedicine, Journal of Strategic Information Systems, International Journal of Production Economics, Drug Discovery Today, and International Journal of Medical Informatics. Her current research interests include strategic management of IT, IT governance, IT security, and healthcare information systems. She was among the top 10 globally in terms of MISQ and ISR publications between 2007 and 2009. She worked for Pharmacia & Upjohn and Kirsch Pharma GmbH for several years. She served as a senior editor for Harvard China Review in 2005-2006.