Journal of the Association for Information Systems

Volume 8 | Issue 7 Article 23

7-6-2007

The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies

Tamara Dinev
Florida Atlantic University, tdinev@fau.edu

Qing Hu
Florida Atlantic University, qhu@fau.edu

Recommended Citation
Dinev, Tamara and Hu, Qing (2007) "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems*, 8(7), .
DOI: 10.17705/1jais.00133
Available at: https://aisel.aisnet.org/jais/vol8/iss7/23

Journal of the Association for Information Systems

JAIS

Research Article

The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies *

Tamara Dinev
Department of Information Technology and Operations Management
Florida Atlantic University
tdinev@fau.edu

Qing Hu
Department of Information Technology and Operations Management
Florida Atlantic University
qhu@fau.edu

Abstract:

While there is a rich body of literature on user acceptance of technologies with positive outcomes, little is known about user behavior toward what we call protective technologies: information technologies that protect data and systems from disturbances such as viruses, unauthorized access, disruptions, spyware, and others. In this paper, we present the results of a study of user behavioral intention toward protective technologies based on the framework of the theory of planned behavior. We find that awareness of the threats posed by negative technologies is a strong predictor of user behavioral intention toward the use of protective technologies. More interestingly, in the presence of awareness, the influence of subjective norm on individual behavioral intention is weaker among basic technology users but stronger among advanced technology users. Furthermore, while our results are consistent with many of the previously established relationships in the context of positive technologies, we find that the determinants "perceived ease of use" and "computer self-efficacy" are no longer significant in the context of protective technologies. We believe that this result highlights the most significant difference between positive technologies and protective technologies: while the former are used for their designed utilities, for which usefulness and ease of use have a significant impact, the latter are used out of fear of negative consequences, for which awareness becomes a key determinant. We discussed the theoretical and practical implications of these findings. The findings of this study extend the theory of planned behavior to the context of protective technologies and shed insights on designing effective information security policies, practices, and protective technologies for organizations and society.

Key Words: Awareness, spyware, technology acceptance, theory of planned behavior, protective technology, behavioral intention.

* This paper was submitted on May 1, 2006 for fast tracking from the 2005 pre-ICIS HCI Workshop. The paper went through two revisions. Dennis Galletta was the accepting senior editor.

Volume 8, Issue 7, Article 2, pp. 386-408, July 2007

1. Introduction

The rampant spread of computer viruses across global networks and frequent security breaches in organizations have elevated the management of information security from the backrooms to the boardrooms of organizations in the global community (Deloitte, 2005). The high level of digital connectivity, powered by innovations in computing and communication technologies, has not only enabled the rapid globalization of economic activities and brought prosperity to communities large and small, it has also created unprecedented opportunities for the dark side of technological advancement to emerge and prosper. Computer viruses, spyware, cyber attacks, and computer system security breaches are daily occurrences. In the ten year period from 1993 to 2003, the number of security incidents reported to CERT increased from 1,334/year to 137,529/year (CERT, 2004). These attacks have resulted in hundreds of millions of dollars in financial losses to U.S. companies and other organizations including government agencies (Gordon et al., 2004, 2005). The losses are much more worldwide (Mercuri, 2003; Cavusoglu et al., 2004). A recent survey of managers in more than 1,300 organizations in 55 countries reveals that the sheer number of security-related regulations and the consequences of non-compliance have led information security to be a top priority in boardrooms (Ernst & Young, 2005).

In order to effectively manage and control the ever-evolving and growing security threats, it is obviously not enough just to rely on deployment of security technologies such as anti-virus and intrusion detection software and hardware. Studies in recent years have repeatedly shown that information security is a socio-technological problem that requires thorough understanding of the weakest link in the defense against security threats: human behavior and attitudes about using these security technologies (Goodhue and Straub, 1991; Straub and Welke, 1998; Dhillon and Backhouse, 2001; Hu et al., 2006). However, research literature that deals with human behavior as it relates to using technologies—such as the literature on innovation diffusion and technology acceptance—is usually concerned with technologies designed or intended to have clearly identifiable benefits for their users. Thus, it is understandable that the extant research is biased toward positive technologies, both within organizations where better job performance is a desirable outcome (e.g. Rogers, 1995; Davis et al., 1989; Igbaria 1994; Gefen and Straub, 1997) and outside organizations where adoption of technologies such as the Internet for e-commerce take place (e.g., Gefen and Straub, 2000; Gefen et al., 2003; Koufaris, 2002; Pavlou, 2003; Pavlou and Fygenson, 2006).

However, the expansion of computer and Internet use in organizations and society at large has also generated many unintended consequences. While individuals, organizations, and society have benefited from the widespread application of information technology (IT), computer users and organizations have become increasingly vulnerable to the threats posed by technologies designed to disrupt or harm systems, individuals, and organizations. The variety and complexity of cyber attacks, viruses, and spyware have grown in parallel to the technologies designed to protect individual users and organizational systems. As more and more security products are developed and deployed, people who wish to use technology for ill-gotten gains seem to find ways to penetrate or bypass these products. As developers strengthen security products in response, the attacks become more sophisticated, creating an ever-escalating and quickening cycle of attack and defense (Bagchi and Udo, 2003; Lipson, 2002).

In this study, we use the term "positive technologies" to refer to those technologies that are designed to benefit their users in terms of productivity, efficiency, competitiveness, or entertainment. On the other hand, "negative technologies" refer to those that are designed to disrupt or harm their users, such as computer viruses, spyware, and tools for breaking into systems and databases. We define "protective technologies" as those that are designed to deter, neutralize, disable, or eliminate the negative technologies or their effectiveness, such as anti-virus software, anti-spyware tools, firewalls, and intrusion detection technologies. Although it can be argued that there is not much difference between positive and protective technologies, since both provide their users a set of utilities, we submit that the ways through which these utilities manifest themselves and the resulting user perceptions of their value are quite different, thus they deserve separate consideration in the context of user technology acceptance research.

Positive technologies, such as office automation applications, enterprise resource planning (ERP) systems, and e-commerce technologies, contribute directly to the productivity and performance of their users and are often viewed as necessary and essential. Protective technologies, on the other hand, contribute to the wellbeing of their users indirectly and subtly and are often viewed by organizational users as extra burdens to the work routine (Hu et al., 2006) and viewed by individual users as annoying (Hu and Dinev, 2005). For example, it is very common that users of process- and resource-intensive applications,

such as image and video processing, digital electronic design tools, or 3D visualization applications, are advised to disable other processes running on their computers, especially anti-virus or anti-spyware tools. Thus, in the mind of an electrical engineer, there is a clear distinction between the positive technology she uses daily to perform her digital design work and the protective technology (anti-virus or anti-spyware program) that she has to turn on and off and may even consider to be impeding her work. It is not an uncommon observation by corporate IT security teams that employees are annoyed and unappreciative when their work is interrupted in order to perform routine security checks of their systems. This important distinction clearly calls for a better understanding of users' attitudes toward and use of protective technologies in work and home environments.

The study of negative technologies is just beginning to emerge (e.g., Bagchi and Udo, 2003; Stafford and Urbaczewski, 2004; Hu and Dinev, 2005). As recognized by Stafford and Urbaczewski (2004), in the case of spyware, little empirical work supports the many suppositions being made about spyware and its effects on personal and business computing. Strong theoretical foundations and empirical validations are still lacking for understanding user behavior in response to negative technologies such as spyware. Fortunately, this situation is changing, and researchers and practitioners have begun to pay more attention to negative technologies, as indicated by a recent special issue of the Communications of the ACM on spyware.

If there is a lack of research on the effect of negative technologies, we submit that there are virtually no studies on user behavior pertaining to protective technologies. In order to design effective policies and practices at the individual, organizational, and societal levels to successfully defend against negative technologies, a thorough understanding of user attitudes and intentions toward and behavior surrounding protective technologies is clearly called for. Given the broad range of protective technologies and their use context, in this study we choose to focus on the attitudes and behavior of *individual* computer users. We are interested in the protective technologies that individuals install and manage on their own systems. Thus, we exclude the category of protective technologies deployed in organizational security network infrastructure (e.g. packet filters, secure routers, second or third generation firewalls, etc.). Additionally, we define use of protective technologies as a user's conscious and voluntary involvement in protecting against negative technologies in the forms of installing, running, and updating protective software tools.

It is important to note that an individual's *conscious* use of protective technologies may vary depending on the usage environment. In many organizations, installations and maintenance of protective technologies (e.g. anti-virus packages and firewall protection) are installed and run automatically on employees' systems and are largely transparent to the end users. In contrast, in some organizations and most homes, where a significant portion of overall computer and Internet use occurs, users are extensively exposed to the threats of various negative technologies, and therefore conscious and active use of protective technologies is critical for the protection of their computers and systems. What makes the matter even more complex is the fact that these two very different environments (home and work) often commingle. More and more users are using computers (including mobile computers) both within the boundaries of an organizational environment where they are fairly well protected by the carefully-designed organizational security policies and technologies and from their homes, where they are also connected to corporate networks via their home computers over which they have complete control about which technologies and what applications to download, install, and use. In addition, many advanced computer users have enough privileges to disable or enable at will various anti-virus or anti-spyware tools running on their work systems. The security and privacy risks in this type of environment are both high and convoluted. Thus, protecting organizational or individual information assets necessarily involves the *conscious* and active use of protective technologies by each employee at work and at home. As a consequence, it is more critical than ever before to understand how users perceive the threats, and how they use protective technologies designed to help them reduce or eliminate the risk.

Thus, in this study, we are interested in addressing the following research questions: What are the factors that influence intentions to use protective technologies and how do they contribute to the formation of this intention? In attempting to answer these questions, we recognize the need to develop a coherent and strong theoretical foundation. We contend that the well-researched user technology acceptance models concerning positive technologies that are either performance- or hedonics-oriented (e.g., Venkatesh et al., 2003; Van der Heijden, 2004) may not fully explain user behavior in the context of protective technologies, where the desired outcome of use is the preservation of the well being of the computer system, i.e., the initial status quo. To understand user attitude and behavior in this context, we draw on the theory of planned behavior (Azjen, 1988) and introduce awareness as a core construct in user behavioral modeling based on the exploratory works of Goodhue and Straub (1991), Stafford and Urbaczewski (2004), and Hu and Dinev (2005).

The rest of the paper is arranged as follows. In section 2, we build our research model and develop our research hypotheses. In section 3, we describe the research methodology, survey instrument, and data collected. In section 4, we present results of a confirmatory factor analysis on the validity of the survey instrument and the results of the structural equation modeling of the proposed user behavioral model surrounding protective technologies. In section 5, we provide

some analyses of the test results and contrast those with the findings in the technology acceptance literature. Finally, in section 6, we summarize the major findings of this study and discuss their theoretical and practical implications.

2. Theoretical Development of Research Model

2.1 Theories of Technology Acceptance

To understand user behavior pertaining to protective technologies, we start with a review of the theory of planned behavior (TPB) (Ajzen, 1988, 2002) and the technology acceptance model (TAM) (Davis, 1989; Davis et al., 1989; Venkatesh and Davis, 2000; Venkatesh et al., 2003), two of the most widely cited theoretical frameworks in the IS literature on user technology acceptance. Both models originate from the theory of reasoned action (TRA) (Ajzen and Fishbein, 1980). TPB contends that a person's behavior is determined by her intention to perform the behavior of interest. This behavioral intention (BI) is, in turn, determined by three factors: attitude toward the behavior (AB), subjective norm (SN), and perceived behavioral control (PBC). AB refers to a person's judgment about whether it is good or bad to perform a behavior of interest. A favorable attitude is likely to encourage individuals to perform the behavior. SN is a person's perception of the social pressure to perform or not perform the behavior in question. SN thus reflects the person's perceptions of whether the behavior is accepted and encouraged by social circles consisting of people who are important to her. Empirical findings in research suggest a positive relationship between SN and BI (e.g., Taylor and Todd, 1995; Karahanna et al., 1999; Venkatesh and Davis, 2000; Venkatesh et al., 2003), however lack of statistical significance between SN and BI has also been reported (e.g. Mathieson, 1991; Pavlou and Fygenson, 2006).

Perceived behavioral control (PBC) is the perceived ease or difficulty of performing a behavior and a personal sense of control over performing it (Ajzen, 1988). PBC is theorized as an antecedent to both intention and behavior (Ajzen, 1988, 2002; Taylor and Todd, 1995; Pavlou and Fygenson, 2006). However, the nature and measurement of PBC has been one of the most controversial issues in TPB (see Pavlou and Fygenson, 2006 for more details). Ajzen later (2002) suggests that self-efficacy (SE) and controllability (C) are separable components of PBC. Self-efficacy is defined as the individual's judgment of his or her skills and capabilities to perform the behavior (Bandura, 1986). Controllability is defined as the individual's judgment about the availability of resources and opportunities to perform the behavior (Ajzen, 2002; Pavlou and Fygenson, 2006). It is a common view that SE reflects internal personality factors, while C reflects beliefs about external factors and resources. While Pavlou and Fygenson (2006) applied SE and C as underlying formative indicators to PBC (PBC treated as a higher order construct), staying faithful to Ajzen's (2002) arguments, SE and C have also been incorporated in Taylor and Todd's (1995) decomposed TPB as distinct constructs influencing PBC in causal relationships. It is worth noting that the conceptualization of SE and C and their relationship to PBC is still debatable (Trafimow et al., 2002).

In response to the limitations associated with TRA (Fishbein and Ajzen, 1975; Ajzen, 1988) in predicting and explaining user acceptance of a new technology, Davis (1989) and Davis et al. (1989) developed TAM as an extension to TRA. Similar to TRA and TPB, the original TAM predicts that attitudes toward a new technology are a factor in its adoption and use. It highlights two key determinants of user acceptance of a new technology: perceived ease of use (PEOU) and perceived usefulness (PU). PEOU is defined as the extent to which the user believes that usage will be effortless. PU is the degree to which a user believes that using the particular technology would enhance her work performance in an organizational context.

While PEOU and PBC are both concerned with the perceived ability to perform a behavior, PEOU is an attitudinal belief about the amount of effort applied, while PBC is a control belief and situational perception. A user of technology might perceive that it is easy to use, but could still feel that she does not have control over the process of use. Ajzen (2002) writes that PBC should be "read as *perceived control over the performance of a behavior*" (p. 668). Pavlou and Fygenson (2006) also found that PEOU influenced PBC (through the underlying dimensions SE and C) in their TPB-based online user behavioral model.

2.2 The Role of Attitude in TAM models

Numerous empirical studies have provided support for TAM (see Venkatesh et al., 2003 for a detailed review). The original TAM (Davis et al., 1989) empirically validated a partial mediation of attitude, while subsequent studies eliminated attitude as a predictor of IT usage (Venkatesh and Davis, 1996; Venkatesh, 1999; Venkatesh, 2000; Venkatesh and Davis, 2000). As a result, the majority of TAM models propose a direct path from PEOU and PU to BI, without attitude as a mediating construct. Most subsequent studies have followed this framework (Gefen and Straub, 1997; Koufaris, 2002; Gefen et al., 2003; Venkatesh et al., 2003; Van der Hejden, 2004). Because TRA and TPB insist that attitude completely mediates the relationships between beliefs and intention, the majority of TAM-related studies therefore contradict the basic principle of TPB and TRA. The explanation found in the extant TAM literature is that, "within organizational settings, people form intentions towards behaviors they believe will increase their job performance, over and above whatever positive or negative

feelings may be evoked toward the behavior per se" (Davis et al., 1989, p. 986). Thus, the direct PU-BI (and PEOU-BI) effect in TAM implies that intentions to use technology may be less affected by the individual's overall attitude toward that technology. In other words, even though an employee may dislike a technology, she may still use it if it is perceived to increase job performance. Furthermore, Venkatesh et al. (2003), in their Unified Theory of Acceptance and Use of Technology (UTAUT) model, have eliminated the role of attitudes by arguing that attitude will not have a direct effect on intention when performance and effort expectancy constructs are included in the model. They consider "any observed relationship between attitude and intention to be spurious and resulting from omission of the other key predictors" (p. 455).

In contrast, Taylor and Todd (1995), in their decomposed TPB model, empirically validated the complete mediation of attitude between PU and PEOU and behavioral intention, as did Bagozzi et al. (1989) and Pavlou and Fygenson (2006). However, the results and explanatory power have been somewhat mixed (see Dillon and Morris, 1996 for a detailed discussion). Models faithful to TPB have exhibited only a moderate increase in explanatory power for intentions. The decomposed TPB adds seven more variables only to increase the predictive power of behavior by 2 percent over TAM (Dillon and Morris, 1996).

Notwithstanding the inconsistencies and contractions among the various models of user technology acceptance, the basic frameworks of TPB and TAM have been shown to be robust in explaining and predicting user behavior toward technological innovations in general, as evident in the sheer number of studies based on these two frameworks.

Despite the major differences between the positive and protective technologies outlined in the previous section, the use of both technologies ultimately brings identifiable benefits to the end user, thus the adoption of both is a desirable outcome. Based on the theoretical review above, we believe that the most theoretically sound approach to investigating the user's conscious behavior toward protective technologies is to adopt the rich framework of TPB, complemented by the two TAM constructs PEOU and PU, as in Pavlou and Fygenson (2006). In the context of protective technology use, we find no strong arguments against the established constructs and relationships in the technology acceptance literature. However, given the unique characteristics of protective technologies, we suspect that many, if not all, of the relationships will change. To test these relationships and to ensure the theoretical completeness and integrity of our research model, we decided to include all TPB-related constructs and relationships as presented in Pavlou and Fygenson (2006) in our research model. In addition, in order to be consistent with both the TPB and the original TAM model (Davis et al., 1989), we treat attitude as a partially mediating variable in the PEOU-BI and PU-BI relationships. However, given the preponderance of the theoretical and empirical studies of these constructs and relationships, we choose not to elaborate on these established relationships as our research hypotheses, though they are included in our research model to preserve the theoretical integrity of the research model. We summarize these relationships in Table 1 and present them in Figure 1.

2.3 Technology Awareness

The concept of awareness first appeared in the innovation diffusion theory (IDT) (Rogers, 1995) and was used as the initial stage of an innovation diffusion process model. According to this theory, innovation diffusion involves two different actors: a company or organization that will adopt the innovation or new technology, and users or individuals who will use the innovation or technology. Further, the decision making process of innovation adoption involves five steps: awareness, attitude formation, decision, implementation, and confirmation. Awareness is defined as the extent to which a target population is conscious of an innovation and formulates a general perception of what it entails. During the awareness stage, an organization or individual is exposed to the existence of the innovation and is provided information on how the innovation functions and what its benefits are. Thus, awareness is an antecedent for the attitude formation stage of innovation diffusion. In the framework of TPB, this would mean that awareness is an antecedent of attitudes and behavioral intentions. Clearly, based on our classification of technologies, awareness in IDT is developed from the perspective of positive technologies.

There are two major differences between the IDT as outlined above and diffusion of the protective technology among individuals not bound within an organization. The first is that there are not two actors but only one – the individual with his or her computer who is solely responsible for deciding whether or not to adopt and use a protective technology. The second difference is that the technology in question is not positive but protective, and as argued in the Introduction, its benefits may not be as clear to the individual. Therefore, we expect that the concept of awareness, although rooted in the IDT, will need to be further developed through the lens of negative technologies and the need for protection and prevention strategies.

Unlike technology innovations and positive technology use in organizations and e-commerce adoption by individuals, the existence of threats from negative technologies is often not known to users because negative technologies are installed surreptitiously and work unnoticed. Also, less known to the users are the strategies and tools for protection from these threats. In many ways, combating negative technologies resembles the fight against disease, crime, and social injustice.

Social and medical sciences have long recognized the importance of raising public and individual awareness in such battles. In the literature of social science, criminal justice, and medical behavioral science (e.g., Snell et al., 1991), the concept of awareness is central to human behavior. Awareness is viewed as one of the key components of consciousness-raising, and brings about an appreciation of the needs, impetus, and specificity of issues, events, and processes. Previous social sciences research defines social awareness as naming the problem, speaking out, raising consciousness, and researching. It is further defined as an individual's active involvement and increased interest in focal issues (Bickford and Reynolds, 2002; Green and Kamimura, 2003; Tillman, 2002). Social awareness has been positively linked to individuals' attitudes and cognitive development (Tsui, 2000; Perry, 1970; Piaget, 1975), and to privacy concerns (Dinev and Hart, 2006).

Following Dinev and Hart (2006), we adopted the concept of awareness of technological issues and define *technology awareness* as a user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them. It is only logical to assume that before an individual can form either positive or negative beliefs about using protective technologies, she must first be made aware of the issues surrounding negative technologies. More specifically, she must be aware of (a) the potential threats and consequences of poor or no protection and (b) the availability and effectiveness of protective technologies. Our broader definition of technology awareness reflects the fact that awareness of a solution is often preceded by awareness of a problem, i.e., there is a need for shields only if there are spears. Support for this conceptualization of awareness that includes problems and solutions, is very well stated by Rogers (1995):

> *…awareness must be initiated by the individual and is not a passive act. Hassinger points out that information about new ideas often does not create awareness, even though the individual may be exposed to this information, unless the individual has a problem or a need that the innovation promises to solve. Perhaps one is faced with a chicken-and-egg type of question. Does a need precede awareness of an innovation or does awareness of a new idea create a need for that innovation? The available research studies do not yet provide a clear answer to this question, but tentative evidence suggests the latter is more common (p.82).*

Negative technologies belong to the class of technologies that have emerged as a problem, a threat, or a "disease" so to speak, as opposed to positive technologies whose developers intend for them to be beneficial to organizations and individuals. In security materials, survey and academic studies, IT executives and security managers talk about the importance of "raising awareness of security threats" (e.g., Deloitte, 2005; Ernst and Young, 2005; Hu and Dinev, 2005; and Hu et al., 2006). A comprehensive "Security Awareness, Training, and Education" program, also known as SETA or SATE, is now widely recommended for securing computer-based resources (NIST SP 800-12, 2006). SETA gives recommendations to maintain a high degree of awareness of the computers' operating state (Stafford and Urbaczewski, 2004). Evidently, "awareness" is already present in the vocabulary of organizations. However, it has yet to be formally conceptualized as a theoretical construct in information security research, with its validity and importance scientifically established.

In the case of individual use of protective technologies, technology awareness is a key factor in understanding user behavior. Goodhue and Straub (1991) were among the first IS scholars who suggested that awareness was an important factor in an individual's belief about information security. They predicted that computer abuse would be a major problem that would not diminish on its own and argued that "a lack of awareness of the danger may lead to weak vigilance by users and greater potential for abuse" (p.14). They argued that "people who are more aware of the potential for abuse would be sensitized to the dangers of inadequate security and would more likely feel that security was unsatisfactory" (p.15). Further they argued that awareness was related to computer literacy and, thus, defined and operationalized awareness as years of experience, managerial level, and user/systems staff status. The authors found weak and partial support of their hypotheses that awareness of technology will result in a higher level of concern for security. They concluded that the likely reason for their result was that the years of experience with information systems was a weak measure of security awareness, injecting additional error and noise into their measurements. Nevertheless, the importance of this study far outweighs those identified weaknesses.

The conceptual treatment of awareness in IDT is different from the one in Goodhue and Straub (1991) and this study. The former focuses on "spreading the word" about a positive product (a specific innovation with a potential to increase productivity), that is already created and ready to be implemented. In the context of Goodhue and Straub (1991) and our study, awareness is not about one product, one application, or one technology. It is knowledge of an existing problem, and potential solutions may or may not exist. In this sense, awareness is closer to situational awareness and problem solving – identifying the problem, speaking out, raising consciousness, and researching solutions to resolve the problem.

Drawing on these prior studies, we argue that the level of technological awareness influences the attitudes and beliefs of users about the need for defending against security threats from negative technologies. Indeed, the more knowledgeable a user is about the problems and consequences of security attacks and the ways to protect against them, the more likely that she will form a positive attitude toward the use of protective technologies. Thus, we propose:

H1: Technology awareness positively influences user attitudes toward using protective technologies.

In addition to the attitude toward behavior, according to TPB, the behavioral norms of an individual user's social group have a strong influence on the behavioral intention of the individual (Ajzen, 1988). However, the behavioral norms of the social group regarding negative or protective technologies are inevitably influenced by its members' awareness of the technologies and their consequences. The process of building awareness of problems is found to guide the development of a social network of organizations that strongly advocates for policies and programs to reduce the problems (Biglan and Taylor, 2000). A critical step in this process is a thorough articulation of the problem achieved through extensive communications to the groups that matter, resulting in stronger group norms (Biglan and Taylor, 2000). In the case of spyware and security breaches that affect Internet users, social networks and groups are likely to be formed by the parties interested in solving the specific problems (Stafford and Urbaczewski, 2004). By building alliances and educating users broadly through the media, these networks could change computer users' group norms regarding tolerance of spyware and other negative technologies. In this process, it is reasonable to argue that the higher the degree of awareness among the members of the social group, the stronger the group norms about using protective technologies. Thus, we propose:

H2: Technology awareness positively influences subjective norms about using protective technologies.

We must note that the relationship between technology awareness (TA) and subjective norm (SN) may have causation leading in both directions. In other words, an established group norm about a certain behavior can, through spreading the word and enhancing communications, affect the level of awareness among individuals in the social group. This dual directionality is similar to the nature of the relationship between SN and PU. For example, it is well established that if a technology is perceived as useful, it will be more likely to be embraced as a norm in a social group, i.e., PU affects SN. However, in their TAM2 model, Venkatesh and Davis (2000) argued the opposite – SN is a determinant of PU in light of the argument that if one's peers have a positive opinion about the usefulness of a technology, one is more likely to form a positive belief about its usefulness as well. In choosing the hypothesized causality between TA and SN, we followed the predominant direction between PU and SN in the literature. Indeed, without members of a social group being aware of a problem or threat, a social norm cannot be established in the first place.

In addition, the literature on TAM presented in Section 2.1 overwhelmingly favors direct links between PEOU/PU and behavioral intention (BI). Using the same logic, we submit that a direct relationship between TA and BI can be supported even more strongly in our research model. The consequences of not using protective technologies—such as identity theft, negative publicity, significant financial loss, and uncertain legal consequences—could be devastating to individuals and organizations. Since such consequences are often reported in the popular media, we argue that awareness alone could motivate a user to take action, regardless of whether he has formed a positive attitude or is influenced by the social group norms. This argument is supported by other studies on crime and disease prevention where heightened awareness directly influences intention to engage in certain behaviors (Carleton et al., 1996; Carlson et al., 1988). Therefore, we propose:

H3: Technology awareness positively influences user intention to use protective technologies.

Integrating the awareness construct and the hypothesized relationships into the well-established TBP theoretical framework yields the research model of this study, as shown in Figure 1. The theoretical and empirical support for the causal linkages in TAM and TPB is readily available in the literature and does not need to be repeated here. However, for the clarity of discussion, we have labeled these relationships R1, R2, … R11, with their main sources listed in Table 1 .

3. Research Methodology and Data

3.1. Anti-Spyware as Protective Technology

Numerous protective technologies exist in organizational and personal computing environments, such as anti-virus, anti-spyware, firewalls, intrusion detection and prevention, encryption, and decryption. In order to empirically test our model of user behavior surrounding protective technologies, we chose anti-spyware, the protective technology that is designed to counter the relatively new, but rapidly expanding, negative technology category of spyware. Spyware has become an epidemic security threat in recent years, allowing an indirect infiltration into computer systems. It is often surreptitiously installed on computers to silently track user computing activities such as web browsing and to sometimes even record

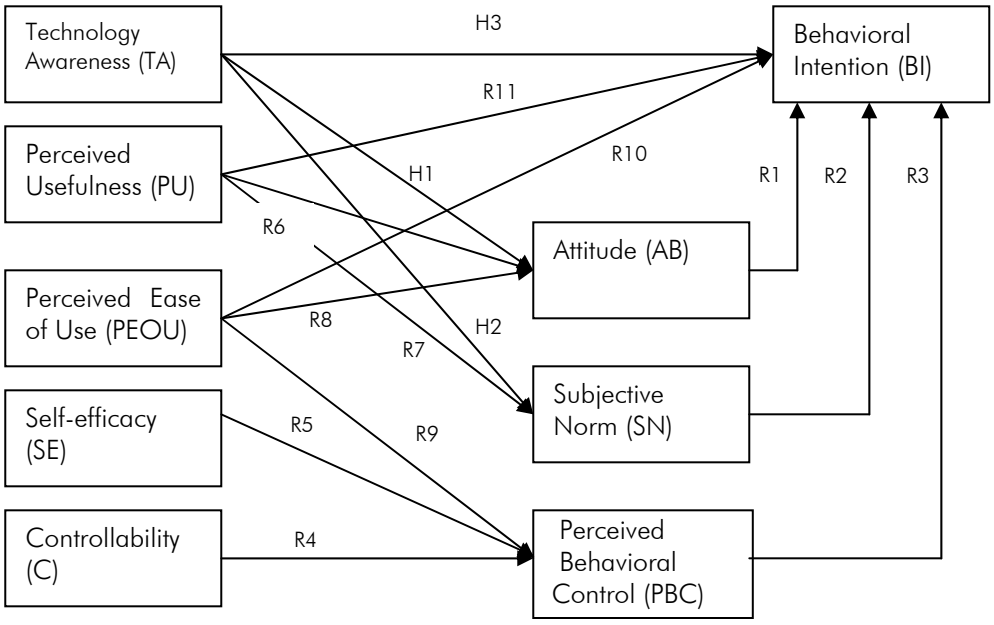

Figure 1: Awareness centric model of user behavior toward protective technologies

Table 1: Summary of the hypotheses and previously established relationships in the research model

Relationships	Description	Source
H1	Technology Awareness -> Attitude toward Behavior	Current study
H2	Technology Awareness -> Subjective Norm	Current study
H3	Technology Awareness -> Behavioral Intention	Current study
R1	Attitude toward Behavior - > Behavioral Intention	Ajzen (1988, 2002), Davis et al. (1989), Taylor and Todd (1995)
R2	Subjective Norm -> Behavioral Intention	Ajzen (1988, 2002), Taylor and Todd (1995), Venkatesh and Davis (2000), Pavlou and Fygenson (2006)
R3	Perceived Behavioral Control -> Behavioral Intention	Ajzen (1988, 2002), Mathieson (1991), Taylor and Todd (1995), Pavlou and Fygenson (2006)
R4	Perceived Controllability -> Perceived Behavioral Control	Ajzen (2002), Taylor and Todd (1995), Pavlou and Fygenson (2006)
R5	Self-Efficacy -> Perceived Behavioral Control	
R6	Perceived Usefulness -> Attitude toward Behavior	Davis et al. (1989), Taylor and Todd (1995), Pavlou and Fygenson (2006)
R7	Perceived Usefulness->Subjective Norm	Venkatesh and Davis (2000)
R8	Perceived Ease of Use -> Attitude toward Behavior	Davis et al. (1989), Taylor and Todd (1995), Pavlou and Fygenson (2006)
R9	Perceived Ease of Use -> Perceived Behavioral Control	Pavlou and Fygenson (2006)
R10	Perceived Ease of Use -> Behavioral Intention	Davis et al. (1989), Venkatesh and Davis (1996), Gefen and Straub (1997), Venkatesh (1999), Venkatesh (2000), Venkatesh and Davis (2000), Koufaris (2002), Gefen et al, (2003), Venkatesh et al. (2003), Van der Hejden (2004)
R11	Perceived Usefulness -> Behavioral Intention	

keystrokes (Doyle, 2003; Taylor, 2002; Stafford and Urbaczewski, 2004). Under the category of spyware several variations exist, such as adware, key loggers, and Trojan horses. Recent media attention to spyware (Cha, 2004; Gutner, 2004; Mitchell, 2004; O'Brien and Hansell, 2004) has revealed that it is often a hidden cost of free access to Internet sites, freeware, and shareware. The danger related to spyware, mainly identity theft (Naraine, 2005), has prompted the government to take action (McGuire, 2004), with Congress passing two bills, the Internet Spyware Protection Act and the Spy Act, which designate installing spyware to break into someone's computer as a federal crime and levy hefty civil penalties.

There are often factors that led us to choose anti-spyware as the representative for protective technologies in this study. Spyware is not created to disrupt or destroy a computer system, but it is designed to function unnoticed by users for as long as possible. It is usually discovered only when too many spyware and adware programs cause sluggish processing, system conflicts, pop-up ads, browser hijacking, and other irritating events on user systems. What makes spyware more dangerous than a virus is how it compromises a user's privacy and could lead to identity theft (Naraine, 2005). The most damaging possibility is that the presence of spyware on corporate desktops could compromise regulatory compliance efforts by leaking private customer data that the corporation is entrusted to protect and, therefore, create legal vulnerabilities (Johnson, 2004). Thus, the impact of spyware on individuals and organizations may be more far-reaching than that of a virus which could paralyze systems in an organization, but only for a short period of time.

Another reason we chose to focus on spyware and anti-spyware is related to the difficulty of raising the awareness of spyware threats among computer users. Because spyware is designed to stay on the computer without causing system disruptions, it can remain undetected and function for long periods of time inconspicuously and surreptitiously. Clearing spyware is often harder than clearing computer viruses from infected systems. In many senses, spyware intrusion is harder to defend against, and disinfection is more complicated than in the case of computer viruses. Sometimes, because of bad programming, but more often intentionally, spyware writes a large number of Windows registry changes, which makes clearing spyware an even more difficult task. In addition, many users seem to accept spyware as the price for getting freeware and shareware from the Internet without being fully aware of the consequences (Delio, 2004; Stafford and Urbaczewski, 2004). In a study released by the National Cyber Security Alliance, a partnership between the tech industry and the Homeland Security Department, an estimated 90 percent of computers using high speed Internet connections collected at least one spyware or adware program (Cha, 2004; Markoff, 2004). Nevertheless, according to studies, spyware seems to generate lackadaisical reactions from Internet users in spite of the predicted dire consequences (Delio, 2004; Roberts, 2004). Consumers continue to use their home PCs for sensitive, online transactions without adequately protecting themselves from potential cyber-crimes (Baig, 2004; Milne et al., 2004). "Most people think they're safe, but they really don't know what's on their computer, and boy, are they vulnerable" (Webb, 2004). User attitudes toward possible identity theft or the compromise of sensitive information due to spyware, security breaches, and other negative technologies strongly resembles the famous "It won't happen to me" attitudes broadly researched and discussed in the crime and disease prevention literature (e.g., Biglan and Taylor, 2000; Boyd and Chubb, 1994; Fried, 1987; Hoffer and Straub, 1989; Hu and Dinev, 2005). Thus, we believe that anti-spyware technologies provide a rich and valid test context for our user behavioral model.

3.2 Construct and Survey Instrument Development

The research model was empirically tested using data collected from a survey developed based on the research model as shown in Figure 1. Measurement items of the survey instrument are provided in Appendix I. The measurements for the TPB constructs—behavioral intention (BI), attitudes toward behavior (AB), subjective norm (SN), and perceived behavioral control (PBC)—as well as measurements for the perceived usefulness (PU), perceived ease of use (PEOU), self-efficacy (SE), and controllability (C), were adapted from existing instruments in the literature and refined through a pilot study. More specifically, we adapted BI, SN, and AB from Taylor and Todd (1995) and Pavlou and Fygenson (2006). We based the measures of PBC on Koufaris (2002) and Taylor and Todd (1995), as well as on the *criterion* items developed by Pavlou and Fygenson (2006) as direct PBC indicators. PU and PEOU were based on Venkatesh and Davis (1996), Taylor and Todd (1995), and Koufaris (2002), C was adapted from Taylor and Todd's (1995) measures of Resource and Technology Facilitating Conditions and Venkatesh (2000). Finally we adapted SE from Bandura (1986) and Pavlou and Fygenson (2006). For each construct, we used two sets of three to four items, one set asking about "cleaning" of spyware, the other about "protecting" against spyware.

It should be noted that we operationalized PBC as a separate construct that mediates the effects of self-efficacy (SE) and controllability (C) on behavioral intention (BI). This is in contrast to Pavlou and Fygenson's (2006) view of PBC as a second-order construct with SE and C as its underlying formative factors. Their approach is in accordance with TPB, where the control belief structures are combined into the *unidimensional* PBC construct (Ajzen, 2002). Such monolithic beliefs, however, pose problems in three aspects: 1) they may not be consistently related to the determinants of behavioral intention

(AB, SN, and PBC) (Taylor and Todd, 1995); 2) these belief sets composed as higher-order unidimensional constructs cannot be analyzed empirically by some of the modern structural equation modeling (SEM) statistical approaches, like LISREL, which makes it difficult to operationalize TPB (Taylor and Todd, 1995; Chin, 1998); and 3) latent variables constructed with formative indicators are not invariant and applicable across various statistical analytical techniques, and testing them or applying them in nomological nets of various models may only be accomplished through partial least squares (PLS). Using formative indicators for latent constructs can generate erroneous and even misleading results when SEM techniques such as LISREL are used, and is viewed as "a common mistake in psychological and sociological journals leading to serious questions concerning the validity of the results and conclusions" (Chin, 1998, p. vii). Attempts to explicitly model formative indicators in an SEM "have been shown to lead to identification problems, with efforts to work around them generally unsuccessful" (Chin, 1998, p. vii).

To address these limitations, Taylor and Todd (1995) introduced the decomposed TPB model, where all the belief structures are decomposed into multidimensional constructs in a way that is consistent and generalizable across different settings and statistical methods, in the spirit of TAM's decomposition of attitudinal beliefs (Davis et al., 1989). In Taylor and Todd's decomposed model, the underlying control belief structure was also decomposed into the original components discussed by Ajzen (1985, 2002): self-efficacy and controllability. For these reasons, in our testing procedure we followed Taylor and Todd's (1995) approach by decomposing all beliefs, including SE and C, and introducing them as antecedents to PBC.

The development of the scales for the new construct introduced in the theoretical model, technology awareness (TA), was initiated by examining prior work on similar constructs in different fields, such as innovation awareness (Rogers, 1995), belief and behavior awareness in sociology (Myers et al., 1996), sexual awareness (Snell et al., 1991; Snell and Wooldridge, 1998), family awareness in psychology (Kolevzon, 1985); situational awareness in cognitive sciences (Adams et al., 1995; Durso and Gronlund, 2000; Endsley, 1995; Sarter and Woods, 1991); medical sciences disease prevention management (Vega et al. 1998), and privacy-related IS research (Dinev and Hart, 2006). The existing social awareness instruments (Green and Kamimura, 2003; Dinev and Hart, 2006) provided important guidance and a base upon which to build. We substantially modified the instruments by deleting, rewording, and adding items. Consistent with current best practices in scale development (Clark and Watson, 1995; Hinkin, 1998; Smith and McCarthy, 1995), we initially cast a wider net of candidate items. Based on an additional search of the Internet and academic, professional, and popular literature, we drafted an initial list of 10 items. We then pilot-tested the instrument for clarity, consistency, and validity with 87 students from the authors' programming classes. Following Churchill (1979), we performed scale purification and refinement, but, in general, the pilot test resulted in only minor changes to the instrument.

Table 2. Demographic Profile of the Survey Respondents

Type	Category	Distribution (%)
Age	<=20	11.7
	21-30	68.4
	31-40	13.9
	>41	6.0
Sex	Male	57.5
	Female	42.5
Major	MIS or Computer Science	47.5
	Other Business Major	49.0
	Other	3.5

3.3 Survey Administration and Descriptive Statistics

We administered the survey instrument to IS professionals and to students of a large Southeastern university to collect data for testing the research model. Students enrolled in various classes were asked to complete the online questionnaire during class time. Alternatively, students who did not have access to computers in their classes were asked to fill out a paper survey. Additionally, we initiated an e-mail campaign with a request for IS professionals who graduated from this university with MIS/CS degrees to participate in this study. We posted links to the online survey on our web sites. Over a period of four weeks, we received 339 responses, of which seven were unusable because of many missing data items. The demographic characteristics of the respondents are shown in Table 2 and Table 3, and the psychometric properties of the awareness construct from the Exploratory Factor Analysis (EFA) stage are shown in Table 4.

Table 3. Computer Skill Profile of the Survey Respondents				
Computer Knowledge ()				
Scale	Overall N=332	MIS/CS N=161	Business N=163	Other N=8
Basic[a]	56.6	34.8	81.0	0
Advanced[b]	23.8	30.4	17.8	14.3
Application development[c]	19.6	34.8	1.2	85.7
Knowledge of Spyware				
Never heard of it	2.7	2.5	3.1	0
Don't know details	16.0	6.9	24.5	28.6
Don't know what to do	26.6	19.4	33.7	28.6
Know what to do	16.3	15.6	16.6	28.6
Fully aware and know how to protect themselves	38.4	55.6	22.1	14.3

a. Basic skills – limited to Word processing, use of e-mail, browsing on the Internet;
b. Advanced computer skills – include basic skills plus ability to manage, configure and install applications;
c. Application development – include advanced skills plus use of programming languages to develop applications.

4. Results and Analyses

4.1 Measurement Validation

We tested the research model through Structural Equation Modeling (SEM) using LISREL. The covariance structure model consists of two parts: the measurement model (sometimes referred to as CFA stage), and the structural model (also known as the SEM stage) (Joreskog and Sorbom, 1989). We used the two-stage approach, as recommended by Anderson and Gerbing (1988), to first assess the quality of our measures through the CFA stage, and then to test the hypotheses through the structural model, the SEM stage. The CFA stage was performed on the entire set of items simultaneously, with each observed variable restricted to load on its *a priori* factor. We conducted all the necessary steps in validation of the measurement model and reliability assessment following the widely used validation heuristics recommended for SEM by Byrne (1998) and Gefen et al. (2000). We found that for each construct, all items from the "cleaning" and "protecting" sets loaded into one common factor. For the parsimony of the study, we reduced the number of items to the generally accepted three, with the exception of the new construct, awareness, for which the final number of items is five.

The analysis resulted in a converged, proper solution with a low χ^2 per degree of freedom and a good fit as indicated by all the listed fit indices. Collectively, the data from the model fit indices (Table 7), factor loadings, and t-values (Table 5) suggest that the indicators account for a large portion of the variance of the corresponding latent constructs and therefore provide support for the convergent validity of the measures (Bollen, 1989; Gefen et al., 2000).

Discriminant validity refers to the extent to which measures of the different model dimensions are unique. It is generally assessed by testing whether the correlations between pairs of dimensions are significantly different from unity (Anderson and Gerbing, 1988). Thus, discriminant validity is supported if the correlations between constructs are not equal or close to 1.00 within 95 percent confidence intervals (Bagozzi, 1991). The highest value of the correlations in our study is .79 between PEOU and PBC with an error term of .04. Thus, with 95percent confidence, the correlation is lying in the interval between .71 and .87. Additionally, discriminant validity can be tested through evaluating pair wise χ^2 difference tests between the constrained (fixed correlation φ_{ij} between two constructs) and unconstrained covariance structures (Segars, 1997; Gefen et al., 2000). In order to establish discriminant validity, the χ^2 value of the unconstrained model must be significantly lower than that of the constrained model. For each model run with a fixed φ_{ij}, the difference in χ^2 was in the tens – considerably greater than the cut-off value of 3.84. Thus, the second and more rigorous technique provided strong evidence for discriminant validity of the measures used in the study. Third, the squared correlations between all latent constructs (Table 6) were significantly less than the corresponding AVE (Fornell and Larcker, 1981). All the criteria adequately demonstrated discriminant validity of the model.

A measure of the internal consistency of the scales is the composite reliability (sometimes called reliability coefficient) computed in conformance with the formula prescribed by Werts et al. (1974). Compared to Cronbach's alpha which provides a lower bound estimate of the internal consistency, the composite reliability is a more rigorous estimate for the reliability (Chin and Gopal, 1995). A composite reliability greater than .5 would indicate that at least 50 percent of the

variance in a measurement is captured by the trait variance and that the variance captured by the measures is greater than the one captured by the errors (Bagozzi, 1991). The recommended values of composite reliability for establishing acceptable model reliability are above .70 (Werts et al., 1974; Gefen et al., 2000) and for establishing strong reliability are above .80 (Koufteros, 1999). The reliability coefficients of the constructs in this study are given in Table 5. The lowest composite reliability is .77, whereas the rest are above .81. The high values of the reliability coefficients provide further evidence of reliability of the scales.

Table 4. Psychometric Characteristics of the Technology Awareness Construct

Item	Mean	Standard Deviation	Corrected Item-Total Correlation	EFA Factor Loadings	Cronbach's α
TA1	2.97	1.12	.69	.81	0.85
TA2	3.23	1.12	.65	.78	
TA3	3.42	1.09	.72	.83	
TA4	3.09	1.12	.62	.76	
TA5	3.74	.98	.60	.74	

Table 5. CFA - Latent Variable Statistics and Psychometric Properties

Latent Variable	Item	Latent Construct Loading and Error term									t-value	Reliability
		BI α =.86	AB α =.92	SN α =.90	PBC α =.86	PEOU α =.84	PU α =.87	TA α =.85	C α =.84	SE α=.86		
Behavioral Intention (BI)	BI1	.81(.04)									14.55	.83
	BI2	.87(.04)									18.58	
	BI3	.67(.04)									20.10	
Attitudes toward Behavior (AB)	AB1		.66(.04)								17.51	.77
	AB2		.76(.03)								22.59	
	AB3		.75(.04)								21.19	
Subjective Norm (SN)	SN1			.89(.04)							20.10	.86
	SN2			.85(.04)							21.24	
Perceived Behavioral Control (PBC)	PBC1				.91(.05)						18.61	.87
	PBC2				.84(.05)						17.81	
Perceived Ease of Use (PEOU)	PEOU1					.71(.05)					13.35	.91
	PEOU2					.95(.05)					17.99	
	PEOU3					.95(.05)					19.18	
Perceived Usefulness (PU)	PU1						.68(.04)				14.75	.81
	PU2						.75(.04)				19.35	
	PU3						.87(.04)				21.97	
Technology Awareness (TA)	A1							.84(.06)			15.21	.93
	A2							.82(.06)			14.64	
	A3							.86(.05)			15.97	
	A4							.74(.06)			12.88	
	A5							.71(.05)			14.22	
Control lability (C)	C1								.99(.04)		22.65	.92
	C2								1.01(.04)		22.42	
	C3								.62(.05)		11.38	
Self-Efficacy (SE)	SE1									.83(.04)	19.85	.94
	SE2									.94(.04)	22.30	
	SE3									.80(.05)	16.40	

Table 6. Latent Variable Statistics*											
	Mean	Std. Dev.	BI	AB	SN	PBC	PEOU	PU	TA	C	SE
BI	3.73	.84	.62								
AB	4.37	.77	.55(.04)	.53							
SN	3.71	.90	.41(.05)	.34(.05)	.76						
PBC	3.28	.64	.43(.05)	.28(.06)	.18(.06)	.77					
PEOU	3.19	.96	.35(.06)	.16(.06)	.20(.06)	.79(.03)	.77				
PU	4.28	.78	.48(.05)	.62(.04)	.50(.05)	.18(.06)	.20(.06)	.59			
TA	3.29	1.42	.66(.04)	.46(.05)	.48(.05)	.40(.06)	.41(.05)	.50(.05)	.63		
C	3.52	.92	.42(.05)	.32(.05)	.38(.05)	.61(.04)	.61(.04)	.43(.05)	.60(.04)	.80	
SE	3.38	.91	.44(.05)	.24(.06)	.36(.05)	.69(.04)	.78(.03)	.35(.05)	.56(.04)	.72(.03)	.79

*The correlations and error terms ( ) are shown in the off-diagonal terms. The diagonal terms indicate the AVE for each construct.

Table 7. CFA and SEM Goodness of Fit Indices										
Goodness of Fit Measures	χ^2 (d.f.)	χ^2/d.f	NFI	NNFI	CFI	IFI	GFI	AGFI	RMR	RMS EA
Good Model Fit Ranges	Non-sign.	<2.00	>.90	>.90	>.90	>.90	≈.90	>.80	<.055	<.800
CFA Model	687.69 (288)	2.39	.90	.93	.94	.94	.88	.83	.056	.065
SEM Model	677.85 (298)	2.27	.90	.93	.94	.94	.88	.83	.052	.062
SEM Model – classic TPB without Awareness (per Pavlou and Fygenson, 2006)	589.75 (193)	3.05	.92	.92	.93	.93	.88	.81	.066	.069

Table 8: Summary of Model Relationships for the whole sample			
Relationship	Description	Statistical Significance	Completely Standardized Path Coefficient
H1	TA - > AB	<0.01	.21
H2	TA - > SN	<0.01	.33
H3	TA - > BI	<0.01	.43
R1	AB - > BI	<0.01	.29
R2	SN - > BI	no	NS
R3	PBC - > BI	<0.01	.16
R4	C - > PBC	<0.01	.29
R5	SE - > PBC	no	NS
R6	PU - > AB	<0.01	.52
R7	PU - > SN	<0.01	.32
R8	PEOU - >AB	no	NS
R9	PEOU - > PBC	<0.01	.61
R10	PEOU - > BI	no	NS
R11	PU - > BI	no	NS

Finally, we addressed the threat of common method bias (Podsakoff et al., 2003; Straub et al., 2004). By ensuring anonymity to the respondents, assuring them that there were no right or wrong answers, requesting that each question be answered as honestly as possible, and providing no incentive for participating in the study, we reduced the likelihood of bias caused by social desirability or respondent acquiescence (Podsakoff et al., 2003). Also, following Podsakoff et al. (2003), we empirically determined the common method variance using Harman's single-factor test by simultaneously loading all items in factor analysis using Varimax rotation. All indicators showed high factor loadings and low cross-loadings. Each principal component explained almost an equal amount of the 72 percent total variance, ranging from 11.4 percent to

17.8 percent. This indicates that our data do not suffer from common method bias.

4.2 Structural Model Testing

The SEM stage specifies the direct and indirect causal relationships among the constructs and the amount of unexplained variance (Anderson and Gerbing, 1988). We report the goodness of fit indices in Table 7. All the values are within an acceptable range for good model fit and, thus, indicate empirical support of the theoretical framework. The structural model (Figure 2) shows the completely standardized parameter estimates among all latent variables. The results provided strong support for the majority of the hypotheses of the study, with most of the path coefficients statistically significant at level .01. Table 8 provides a summary of the support of the hypotheses.

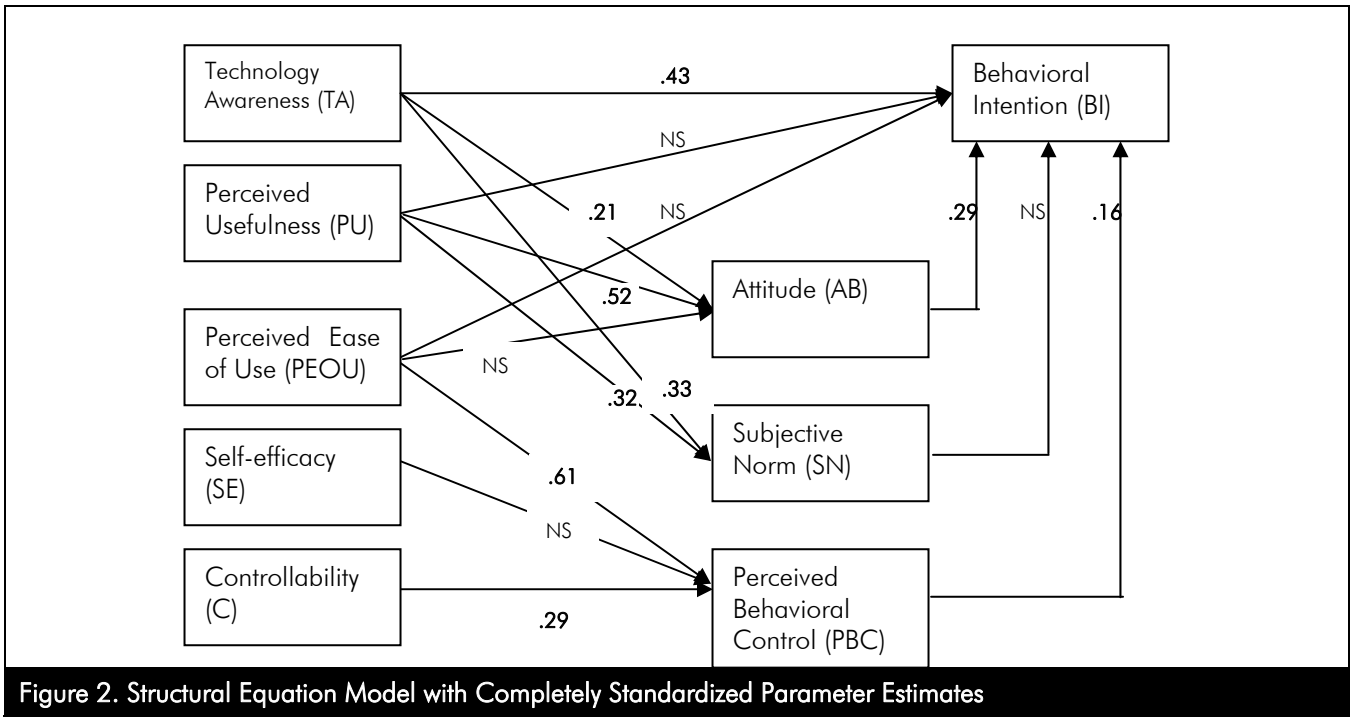

Figure 2. Structural Equation Model with Completely Standardized Parameter Estimates

* (Bold denotes statistical significance at level p<.01. NS = not statistically significant.)

5. Discussion and Post-Hoc Analysis

The empirical results of our study rendered clear support for its core hypotheses: the centrality of technology awareness in the formation of user attitudes toward and behavior surrounding usage of protective technologies, in this case, anti-spyware. Additionally, a strong correlation exists in our model between awareness and all of the other belief constructs included (see Table 6, shaded row). Indeed, higher awareness and conscious knowledge of the need to use protective technologies affect the perception of their usefulness (PU) and are related to the perception of ease of use (PEOU). Similarly, higher awareness increases users' confidence that they can successfully prevent negative technologies in their system (SE), as well as their belief that they has the skills and tools (C) to successfully combat the effects of negative technologies through the use of protective technologies.

Furthermore, the previously well-established relationships between the major constructs of TPB and TAM in the context of positive technologies were largely reconfirmed in the context of protective technologies, suggesting strong generalizability and robustness of the TPB theoretical framework. However, there are some notable exceptions. Some of the previously established TPB and TAM relationships were not found to be statistically significant in our data. These relationships involve perceived usefulness (PU), perceived ease of use (PEOU), subjective norm (SN), and self-efficacy (SE). Because the measurement instruments used for these constructs have been tested and validated in current and previous studies, we are confident that these findings were not due to measurement error. Hence, we believe that there are theoretical reasons for the lack of statistical significance in those relationships. In particular, we believe that they reflect the specificity of the technologies in question – protective technologies that have no immediate benefit for the users in terms of job performance or job satisfaction and, therefore, do not manifest their usefulness and ease of use directly and positively, as is often the case in the context of positive technologies.

The insignificance in the relationship between PEOU and AB (R8) could be attributed to the phenomenon that a user may use a protective technology not because he or she likes it but because he or she perceives there is a real threat to the

computer and/or the personal information it contains. In that sense, the perceived ease of use is less likely to affect his or her attitude toward using the technology. This is analogous to a medical situation where whether an individual feels that a protective measure such as an exam or a procedure is *easy* or not has little to do with his or her attitude toward going to the office to be examined or treated. The individual feels compelled to use protective measures as long as he or she perceives that the technology or treatment is *useful*, regardless of whether it is *easy to use*.

A similar argument can be made about the diminished influence of self-efficacy on perceived behavioral control (R5). An individual may feel compelled to use anti-spyware or anti-virus technologies regardless of how much confidence she or he has in using them. Again, the awareness of the threat is a compelling enough reason to act, even if it means that one has to struggle to get it right. The lack of statistical significance of SE on PBC in our study adds to the surrounding controversy about the nature and measurement of PBC and its components SE and C and may illuminate further research efforts.

The direct link of PEOU and PU on BI (R10 and R11), in accordance with the majority of the TAM models, was not supported in our study. Neither relationship was statistically significant, making TA the only belief construct that has a direct effect on BI (H3). The data seem to suggest that in the case of using protective technologies, just the perception of usefulness or ease of use is not enough to motivate users to act. Rather, it is the awareness of the consequences of not using the technologies that motivates users to act, regardless of other attitudes and control beliefs. This result highlights the most significant difference between positive technologies and protective technologies: while people use positive technologies for their designed utilities on which PU and PEOU will have a significant impact, they use protective technologies mainly out of fear of the consequences of not using them. In fact, this finding is quite consistent with prospect theory (Kahneman and Tversky, 1979), which suggests that people are more inclined to avoid losses than to pursue gains.

The lack of statistical significance between SN and BI (R2) renders mixed results with regard to the core concept of TPB. While several other TPB-based studies found similar lack of support (Mathieson, 1991; Pavlou and Fygenson, 2006), we believe that, in the context of our study, and given the importance of social pressure in dealing with threats and social problems in general, it is harder to explain without a further analysis of the empirical data. For that purpose, we ran a model excluding the awareness construct, reducing it to the ones previously reported in the literature (e.g., Pavlou and Fygenson, 2006). The new model preserved the essence of all other relationships (including the lack of statistical significance between PEOU and AB, SE and PBC, PU and BI, and PEOU and BI) except for the SN-BI link, which became statistically significant at level .01 with a path coefficient of .19. Testing this alternative model was important for three reasons. First, it reproduced and, thus, validated our empirical results with respect to the previously published models. Second, the fit indices of the alternative model were lower (Table 7), with χ^2/d.f. significantly higher than our SEM model indicating that the latter indeed described better the empirical data. Third, the change of the SN-BI relationship confirmed the importance of the direct relationship between technology awareness and behavioral intention (H3). Without the awareness construct present in the model, SN becomes a dominant construct and renders a statistically significant effect on BI.

The above argument, however, does not explain why the importance of the subjective norm on behavioral intention is diminished in the presence of the awareness construct. Our expectations were that an increased awareness, through its strong effect on SN a*nd* through the strong effect of SN on BI, would strongly influence BI both indirectly and directly. After all, raising the awareness of a problem should heighten the sense of urgency in an individual's social circles about taking action, and in doing so, influence the individual's own behavior. To understand the nature of the SN-BI relationship better, we performed a multi-group analysis on two distinguishable groups that constituted our sample: 161 respondents with MIS/CS degrees or majors (i.e. advanced IT users), and 163 respondents with other business degrees (i.e. basic IT users). The computer skills of the two groups are shown in Table 2. After validating the instrument items by establishing convergent and discriminant validity and reliability for each group, we proceeded to test the model separately for each group. Four of the path coefficients proved to be statistically different between the two groups, as established by the χ^2 difference test. The differences are given in Table 9.

Table 9. Path Coefficients for Each Group *

Relationship	Description	Advanced IT Group	Basic IT Group	Full Sample
R2	SN-BI	.23	NS	NS
R7	PU-SN	NS	.58	.32
H3	TA-BI	**.11**	.52	.43
R3	PBC-BI	.27	NS	.16

*All path coefficients are significant at level .01, except for NS (not significant) and the bold which is significant at level .05.

It is immediately clear that the influence of subjective norm (SN) on behavioral intention (BI) (R2) is stronger for the advanced IT group than for the basic IT group. We believe that the advanced IT group is more cohesive than the basic IT group, and individuals communicate to a greater extent about IT-related issues and are keen to learn what their peers are using to solve a problem. Thus, the influence of peers on individual behavior tends to be stronger in the advanced IT group than in the basic IT group. In the advanced IT group, the greater awareness they have, the more they tend to discuss and seek solutions within their social circles, exchange know-how and ideas. In contrast, awareness appears to inspire action rather than communication in the basic IT group, as shown by the significantly larger TA-BI (H3) relationship. Due to the loose ties among the members who were from a variety of majors in different colleges, we assume there was little discussion about computer technologies, thus their social circles exerted minimal influence on how to react to a cyber threat such as spyware. One implication of this finding is that an effective approach to reach socially diverse groups is to establish pro-active social networks to educate and advocate the necessity to protect against certain threats, such as negative technologies.

The weaker (or lack of) influence of PU on SN (R7) for the advanced IT group can also be explained by the characteristics of the two groups. Advanced IT users are more prone to experiment with a technology even if its usefulness is in doubt. Thus, mere suggestions to use or try a tool, especially if it deals with security and protecting one's computer, might influence advanced IT peers much more than basic IT users who may need first to be convinced that the tool is useful before feeling social pressure .

The weaker relationship between TA and BI (H3) for the advanced IT group can be attributed to the stronger SN influence on BI for that group. Indeed, because basic IT users do not tend to discuss technology-related issues as much as advanced IT users, being aware of a problem may inspire them to act, while the members of the advanced IT group may weigh their peers' opinion more heavily before acting.

Finally, we shall note that for the basic IT group, PBC does not have a significant effect on behavioral intention (BI) (R3). This may be attributed to the characteristics of the basic group, as discussed above. We suspect that individuals in the basic IT group perceived little sense of control when dealing with viruses or spyware threats and computer technologies in general, as evidenced by the low level of mean value of PBC for the basic IT group: 1.7 versus 3.2 for the advanced IT group. The subsequent t-test confirmed that the difference was significant. This was consistent with previous discussions about the behavior of basic IT users. They seemed to be influenced more by fear as the result of awareness and less by utility of the protective technologies.

6. Theoretical and Practical Implications

Our findings have both theoretical and practical implications. Theoretically, we found that in the context of using protective technologies, some of the previously-established important relationships between user behavior and positive technologies no longer hold. In the presence of threats from negative technologies, it is fear of the dire consequences of not using protective technologies that motivates people to act. In dealing with negative technologies, conventional motivational factors such as perceived usefulness (PU) and perceived ease of use (PEOU) become less meaningful or at least less significant. Instead, awareness was shown to be particularly salient in understanding the user behavior pertaining to protective technologies. The extended theory of user behavior presented in this study, however, is not limited to protective technologies. We submit that it is possible to generalize the findings to other classes of technologies, including those that are utilitarian and hedonic. Indeed, awareness of any technologies or awareness of problems and the ways to resolve the problems might be central to a broad spectrum of innovations at individual and organization levels.

In practical terms, our findings provide insights for managers to design more effective security policies and practices to work in conjunction with technologies in the fight against the onslaught of spyware and other Internet-spawned negative technologies. For example, in order to reach average computer users, it is important to create social advocacy groups and networks that educate and raise awareness about protecting personal computer systems from the potential threats of negative technologies. If these users do not belong to more cohesive IT-related social circles, traditional information channels, such as television or news pages, could play an important role in developing social pressures and advocating policies that address and compel protection and prevention of computer systems in a globally connected society. In that sense, our research findings provide timely guidance and validation for what practitioners have already initiated in their attempts to motivate computer users to take action against negative technologies. For example, Internet providers, software companies, and computer makers are making an effort to increase awareness of threats and provide customers with user-friendly tools to protect themselves. Prominent information technology companies and computer makers (e.g., Dell, Microsoft, Verizon, Amazon, AT&T, AOL, Yahoo) have launched a non-profit Internet Education Foundation to help consumers combat spam and spyware (Bridis, 2004). In terms of designing effective training programs for information security, our findings suggest that just teaching users how to use protective technologies is not enough; security managers

and trainers should allocate enough time to convey the consequences of not protecting one's computer and data. For developing corporate security policies and procedures, our results suggest that deterrence against violations of procedures should be articulated clearly in policies, and firms should make sure that employees are fully aware of the consequences of non-compliance.

If we were to use one metaphor for our findings, it would be disease prevention. According to Carleton et al. (1996, Table 1), "[I]ncreased awareness is often a necessary first step before behavioral change," a finding also supported in our study through the direct relationship between TA and BI. Further, they report that "many respondents already have a high level of awareness and knowledge but lack the skills for, or need additional information on, how to make behavioral changes." This finding is also confirmed by our results, because, in addition to awareness, other factors like perceived behavioral control and subjective norms also contribute to a behavior. The authors recognize that "acceptance of programs is also influenced by cultural norms" – a finding that is crucial in our model, through the subjective norm construct. Another finding, not captured in our study, is that "the benefits of awareness and knowledge programs are dependent on the readiness of the audience to learn and individual learning styles." We consider examining readiness to learn and individual learning styles as an important potential future addition to our model.

7. Conclusions

In this paper, we introduced and studied the role of technology awareness in forming an individual's intention to use protective technologies, defined as computer technologies that protect data and systems from viruses, unauthorized access, disruptions, spyware, and other negative technologies designed to affect or disrupt computer systems and the individuals using them. Drawing on the extant literature, we defined *technology awareness* (TA) as the user's raised consciousness of and interest in knowing about technological issues and problems and strategies to deal with them. We then integrated this construct in the nomological net of TPB and TAM variables to empirically test a model of user behavioral intention, specifically in the context of use of protective technologies. The study's results confirmed the theoretical arguments that TA is a central determinant to the formation of a user's behavioral intention to use protective technologies. TA was shown to strongly influence attitudes toward behavior, subjective norm, and behavioral intention. We also found that awareness is highly correlated with the TPB and TAM beliefs such as perceived controllability, self-efficacy, perceived ease of use, and perceived usefulness.

There are certain limitations of the study that may also inform a number of possibilities for future research on awareness and user behavior pertaining to protective technologies. First, the study's results regarding perceived behavioral control and its antecedents (self-efficacy and controllability) showed the complex nature of the construct. The treatment we adopted could be debatable and warrants further exploration. Second, we acknowledge that the technology awareness construct might not be specific enough to the behaviors in our operationalization. We adopted a broader definition of awareness, while its evidently multidimensional nature could call for a more refined approach. Future refinement of the construct could distinguish between awareness of a problem and awareness of a solution to that problem. An integrative, multidimensional approach to awareness could enrich the findings of the current study. For example, Biglan and Taylor (2000) argue that the process of building awareness about a certain issue involves an analysis of the issue that articulates (a) the harms associated with its presence, (b) the causes of its presence, and (c) the programs and policies that could reduce its presence. Therefore, future multidimensional approaches could involve the diagnostic and control components as an underlying causal mechanism, along with personal risk aversion, past experience of security violations, and experience with computers. With respect to the latter, group differences between basic and advanced IT users observed in the current study's post-hoc analysis should be theoretically explored in a future expanded model. Another potential research direction is to expand the current study on why some users exhibit the "won't happen to me" philosophy, i.e., even being aware of the negative consequences, some individuals still accept the presence of the negative technologies as the "price" of working with computers and being connected to the Internet.

Furthermore, our data were gathered from a more or less convenient sample, which may be biased toward college-age computer users. Future studies could expand the sample to include a more diversified demographic population. Finally, an important future research direction could be to study how awareness impacts other constructs studied within the TPB and TAM frameworks. Our current study focused on validating the construct of awareness and its impact on user behavioral intentions. However, more theoretical insights could be ascertained by examining how the addition of awareness alters the relationships between other established constructs in the TPB and TAM model in various contexts.

Notwithstanding these limitations, we hope our study has made a clear distinction among positive, negative, and protective technologies and called for the attention of IS researchers to the unique issues involved in the acceptance of protective technologies at both individual and organizational levels. By arguing that awareness plays a central role in the acceptance

of protective technology, we believe that the theoretical framework for user behavior surrounding technology and the management practices related to information security can be further advanced by this and future research.

Acknowledgements

An earlier version of this paper was presented to the pre-ICIS HCI workshop on December, 2005. The authors want to thank the anonymous reviewers whose extensive and excellent comments had enormously helped the paper in every aspect and clarified definitions, perspectives, and theoretical arguments. We also want to thank Dennis Galletta for his valuable guidance, promptness, energy, and willingness to work with us in steering the manuscript towards successful publication. We also thank the reviewers of our submission to the HCI workshop, as well as Paul Lowry who served as the SE of the workshop, and the participants of the workshop. The perspectives and the positioning of our paper all benefited from their valuable feedback and comments, and we believe they all contributed to the improvements which permitted the work's publication.

References

Adams, M.J., Tenney, Y.J., and Pew, R.W. 1995. Situation awareness and the cognitive management of complex systems. *Human Factors*, *37*, 85–104.

Ajzen, I. 1988. Attitudes, Personality, and Behavior, The Dorsey Press, Chicago, IL 60604.

Ajzen, I. 2002. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology, 32*, 665-683.

Ajzen, I. and Fishbein, M. 1980. Understanding Attitudes and Predicting Social Behavior, Prentice-Hall, Englewood Cliffs, NJ.

Anderson, J. C., and Gerbing, S. W. 1988. Structural Equation Modeling in Practice: a Review and Recommended Two-Step Approach, *Psychological Bulletin* , 103, 3, 411-423.

Bagchi, K. and Udo, G. 2003. An Analysis of the Growth of Computer and Internet Security Breaches, *Communications of the Association for Information Systems*, 12, 684-700.

Bagozzi, R. 1991. Structural Equation Models in Marketing Research, *I st Annual Advanced Research Techniques Forum,* ed. W. Neil, Chicago: American Marketing Association, p. 335.

Bagozzi, R.P., Baumgartner, J., and Yi., Y. 1989. An Investigation into the Role of Intentions as Mediators of the Attitude-Behavior Relationship. *Journal of Economic Psychology,* 10, 35-62.

Baig, E. C. 2004. Keep spies from skulking into your PC, USA Today, January 22.

Bandura, Albert. 1986. *Social foundations of thought and action: A social cognitive.* Englewood Cliffs, NJ: Prentice Hall.

Biglan, A. and Taylor, T.K. 2000. Why Have We Been More Successful in Reducing Tobacco Use Than Violent Crime? *American Journal of Community Psychology*, 28, 3, 269 – 302.

Bickford, D. M. & Reynolds, N. 2002. Activism and service-learning: reframing volunteerism as acts of dissent. Pedagogy, *Critical Approaches to Teaching Literature, Language, Composition and Culture*, 8, 2, 229-252.

Bollen, K. 1989. *Structural Equations with Latent Variables*, Wiley, New York, N.Y.

Boyd, M. and Chubb A. 1994. Health Visiting A New Model for a Deprived Area, *International Journal of Health Care Quality Assurance*, 7, 5, 8-11.

Bridis, T. 2004. Group, Dell Launch Anti-Spyware Campaign, *USA Today*, October 16. Accessed on May 1 at http://www.usatoday.com/tech/news/internetprivacy/2004-10-16-dell-anti-spyware_x.htm .

Byrne, B. 1998. *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS*, Lawrence Erlbaum Associates, N.J.

Carleton R.A., Bazzarre, T., Drake, J., Dunn, A., Fisher, E. B. Jr, Grundy, S.M., Hayman, L., Hill, M.N., Maibach, E.W., Prochaska, J., Schmid, T., Smith, S.C. Jr, Susser, M.W., and Worden, J.W. 1996. Report of the Expert Panel on Awareness and Behavior Change to the Board of Directors, American Heart Association, *Circulation*, 93, 9, 1768 - 1772. Available at http://circ.ahajournals.org/cgi/content/full/93/9/1768 .

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. A model for evaluating IT security investments. *Communications of the ACM*, 47(7), 87-92.

Carlson M, Charlin V, Miller N. J. 1988. Positive mood and helping behavior: a test of six hypotheses, *Perspectives of Social Psychology,* 55, 2, 211-29.

CERT. 2006. *CERT/CC Statistics 1988-2006.* 2004. CERT Coordination Center. Available online at http://www.cert.org/stats/cert_stats.html. Last accessed on April 28, 2006

Cha, A. E. 2004. Computer Users Face New Scourge, Washington Post, October 10, p. A01.

Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling. *MIS Quarterly,* 22(1), pp. vii – xvi

Chin, W., A. Gopal. 1995. Adoption intention in GSS: Importance of beliefs, *Data Base Adv.* 26 42-64.

Churchill, G. 1979. A Paradigm for Developing Better Measures of Marketing Constructs, *Journal of Marketing Research,* 16, 1, 64-73.

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

Davis, F. D. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology *MIS Quarterly*, 13, 319-340.
Davis, F. D.; Bagozzi, R. P.; Warshaw, P. R. 1989. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, *Management Science*, 35, 8, 982-1003.
Delio, M. 2004. Spyware on my machine? So what? Wired News, December 06, 2004.
Deloitte. 2005. Global Security Survey, Deloitte Touche Tohmatsu. Available online at http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritySurvey_2005-07-21.pdf. Last accessed on April 26, 2006.
Dhillon, G. and Backhouse, J. (2001) "Current Direction in IS Security Research: Towards Socio-Organizational Perspectives," Information Systems Journal, 11, 127-153.
Dillon, A. and Morris, M. 1996. User acceptance of information technology: theories and models. In: M. Williams (ed.), *Annual Review of Information Science and Technology*, Vol. 31, pp 3-32. Medford, NJ: Information Today.
Dinev, T. and Hart, P. 2006. Internet privacy concerns and social awareness as determinants of intention to transact, *International Journal of E-Commerce*, 10, 2, 7-31.
Doyle, E. 2003. Not All Spyware is as Harmless as Cookies: Block it or Your Business Could Pay Dearly, *Computer Weekly,* November 25, p. 32.
Durso, F. and Gronlund, S. 2000. Situation Awareness, in F. Durso et. al. (eds.) *Handbook of Applied Cognition.*, 283-314, NY: Wiley.
Endsley, M. 1995. Measurement of Situation Awareness in Dynamic Systems. *Human Factors* 37, 1, 65-84.
Ernst and Young, 2005. Global Information Security Survey 2005: Report on the Widening Gap. EYGM Limited.
Fishbein, M., Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Addison-Wesley, Reading, MA.
Fornell, C., D. F. Larcker. 1981. Evaluating structural equation models with unobservable measurement error *J. of Marketing Res.* 18 39-50.
Fried, R.A. 1987. The family physician and health objectives for the nation, *Journal of Family Practice*, 3, 296–302.
Gefen, D. and Straub, D.W. 1997. Gender Differences in the Perception and Use of E-Mail: An Extension to the Technology Acceptance Model, *MIS Quarterly*, 21, 4, 389-400
Gefen, D. and Straub, D.W. 2000, The Relative Importance of Perceived Ease-of-Use in IS Adoption: A Study of E-Commerce Adoption, *Journal of the Association for Information Systems*, 1, 8, 1-30.
Gefen, D., Straub, D. W., Boudreau, M.C. 2000. Structural Equation Modeling And Regression: Guidelines For Research Practice, C*ommunications of AIS* , 4, Article 7.
Gefen, D., Karahanna, E. and Straub, D.W. 2003. Trust and TAM in Online Shopping: An Integrated Model', *MIS Quarterly*, 27, 1, 51-90
Goodhue, D.L. and Straub, D.W. 1991. Security concerns of system users: A study of perceptions of the adequacy of security, *Information & Management,* 20, 13-27.
Gorden, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2004) "2004 CSI/FBI Computer Crime and Security Survey," Computer Security Institute. Available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf, accessed on July 25, 2006.
Gorden, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2005) "2005 CSI/FBI Computer Crime and Security Survey," Computer Security Institute. Available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf, accessed on July 25, 2006.
Green, S. P., Kamimura, M. 2003. Ties that bind: enhanced social awareness development through interactions with diverse peers, *Annual Meeting of the Association for the Study of Higher Education*, Portland, Oregon.
Gutner, T. 2004. What's lurking in your PC? *BusinessWeek*, October 04.
Hinkin, T. R. 1998. A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods*, 1, 1, 104-121.
Hoffer, J.A. and Srraub, D.W. 1989. The 9 to 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review,* 30, 4, 35-44.
Hu, Q. and Dinev, T. 2005. Is Spyware an Internet Nuisance or Public Menace? *Communications of the ACM,* 48, 8, 61-66.
Hu, Q., Hart, P., and Cooke, D., 2006. "The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective," Proceedings of the 39th Hawaii International Conference on Systems Science (HICSS 39), January 4-7, Hawaii, USA. CD-ROM, IEEE Computer Society.
Igbaria, M. 1994. An examination of the factors contributing to microcomputer technology acceptance, *Accounting, Management and Information Technologies*, 4, 4, 205-224.
Johnson, M. 2004. Spyware wake-up call, *Computerworld*, May 03.
Joreskog, K. and Sorbom, D. 1989. *LISREL 7 User's Reference Guide*, Scientific Software, Chicago, IL.
Kahneman, D, and Tversky, A. 1979. Prospect Theory: An Analysis of Decision under Risk, Econometrica, XVLII, 263-291.

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. *MIS Quarterly,* 23, 2, 183-213.
Kolevzon, M.S., Green, R.G. 1987. Family awareness scales [FAS], IN: Corcoran K & Fischer J. *Measures for clinical practice: A sourcebook*. New York: Free Pr., 436-439.
Koufaris, M. 2002. Applying the Technology Acceptance Model and Flow Theory to Online Consumer Behavior, *Information Systems Research,* 13, 2, 205-223.
Koufteros, X. A. 1999. Testing a model of full production: a paradigm for manufacturing research using structural equation modeling. *Journal of Operations Management* 17, 467-488.
Lipson, H. F. (2002) Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. CERT Coordination Center Special Reprot CMU/SEI-2002-SR-009. Available online at http://www.cert.org/archive/pdf/02sr009.pdf. Last accessed on April 29, 2006.
Markoff, J. 2004. Home Web Security Falls Short, Survey Shows. *New York Times*, October 25.
Mathieson, K. 1991, Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior, *Information Systems Research*, 2, 3, 173-191.
McGuire, D. 2004. FTC Sues Spyware Suspects, Washington Post, October 12.
Mercuri, R. T. 2003. Analyzing Security Costs. Communications of the ACM, 46, 6, 15-18.
Milne, G. R., Rohm, A. J., Bahl, S. 2004. Consumers' Protection of Online Privacy and Identity, *Journal of Consumer Affairs*, 38, 2, 217.
Mitchell, R. L. 2004. Spyware sneaks into the desktop, Computerworld, May 03. Retrieved at http://www.wired.com/news/technology/0,1282,65906,00.hml.
Myers L.J., Montgomery D., Fine M., Reese R. 1996. Belief and behavior awareness scale [BABAS], IN: Jones RL. *Handbook of tests and measurements*. (2 Vols). Hampton, VA: Cobb & Henry Publishers. V.2, 19-36.
Naraine, R., 2005. Spyware Researchers Discover ID Theft Ring, eWeek, August 8. available at http://www.eweek.com/article2/0,1895,1845248,00.asp
NIST (National Institute of Standards and Technology). 2006. Special Publication SP 800-12. Chapter 13: Awareness, Training, and Education. available at http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter13.html
O'Brian T. L. and Hansell, S. 2004. Barbarians at the Digital Gate, *New York Times*, Sep. 19.
Pavlou, P. A. 2003. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model, *International Journal of Electronic Commerce*, 7, 3, 101-34.
Pavlou, P. A. and M. Fygenson (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly*, 30, 1, 115-143.
Perry, W. 1970. *Forms of Intellectual and Ethical Development in The College Years: A Scheme*, Holt, Rinehart & Winston, New York.
Piaget, J. 1975. *The Equilibrium Of Cognitive Structures: The Central Problem Of Intellectual Development*. University of Chicago Press, Chicago.
Podsakoff, P. M., MacKenzie, S. B., Lee, J-Y., 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, 879-903.
Roberts, P. 2004. AOL survey finds rampant online threats, clueless users, Computerworld, October 25.
Rogers, E. M. 1995. *Diffusion of Innovations*, 4th Edition, Free Press: New York, NY.
Sarter, N. and Woods, D. 1991. Situation Awareness: A Critical but ill-defined Phenomenon. *International Journal of Aviation Psychology* 1, 45-57.
Segars, A. H. 1997. Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems Research, *Omega* 25, 1, 107-121.
Sia, C-L., Lee, M. K. O., Teo, H.-H., and Wei, K.K., 2001. Information Instruments for Creating Awareness in IT Innovations: An Exploratory Study of Organizational Adoption Intentions of ValuNet, *Electronic markets*, , 11, 206-215.
Smith, G. T. and McCarthy, D. M. 1995. Methodological considerations in the refinement of clinical assessment instruments. *Psychological Assessment*, 7, 3, 300-308.
Snell, W. E., Jr., Fisher, T. D., and Miller, R. S. 1991. Development of the Sexual Awareness Questionnaire: Components, reliability, and validity. *Annals of Sex Research*, 4, 65-92.
Snell, W. E., Jr., & Wooldridge, D. G. 1998. Sexual awareness: Contraception, sexual behaviors and sexual attitudes. *Sexual and Marital Therapy*, 13, 191-199.
Stafford, T. F. and Urbaczewski, A. 2004. Spyware: The Ghost in The Machine, *Communications of the Association for Information Systems,* 291-306.
Straub, D. W. and Welke, R. J. 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 22, 4, 441-469.
Straub, D., Boudreau, M.-C., and Gefen, D. 2004. Validation Guidelines for IS Positivist Research. *Communications of AIS,* 13, Article 24, 380-427.

Journal of the Association for Information Systems

Taylor, C. 2002. What Spies Beneath, *Time*, 160, 15, p. 106.
Taylor, S. and Todd P.A. 1995. Understanding Information Technology Usage: A Test of Competing Models, *Information Systems Research,* 6, 3, 144-176.
Terry, D. J. and O'Leary, J. E. 1995. The Theory of Planned Behaviour: The Effects of Perceived Behavioural Control and Self-Efficacy, *British Journal of Social Psychology*, 34, 199-220.
Tillman, B. 2002. Internet privacy legislation emerges: new legislation could bring U.S. privacy protection laws into step with those of the European Union. (Legislative & Regulatory Update). *Information Management Journal*, 36, 5, 14-18.
Trafimow, D., Sheeran, P., Conner, M., and Finlay, K. "Evidence that Perceived Behavioral Control is a Multi-Dimensional Construct: Perceived Control and Perceived Difficulty" *British Journal of Social Psychology* 41, 1, 2002, 101-121.
Tsui, L. 2000. Effects of campus culture on students' critical thinking. *The Review of Higher Education*, 23, 4, 421-441.
Van der Heijden, H. 2004. User Acceptance of Hedonic Information Systems. *MIS Quarterly*, 28, 4, 695-704.
Venkatesh, V. 1999. Creation of Favorable User Perceptions: Exploring the Role of Intrinsic Motivation, *MIS Quarterly,* 23, 2, 239-260.
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, 342-365.
Venkatesh, V., and Davis, F. D. 1996. A Model of the Perceived Ease of Use Development and Test, *Decision Sciences,* 27, 3, 451-481.
Venkatesh, V., & Davis, F. D. 2000. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46, 2, 186-204.
Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27, 3, 425-478.
Vega WA., Sallis JF, Patterson T, Rupp J, Atkins C., Nader PR. 1998. Adult health behavior knowledge scale [HCAT] (1987) & child health behavior knowledge scale [HCAT] IN: Redman BK. *Measurement tools in patient education.*, 49-56, New York: Springer Pub. Co.
Webb, C. L. 2004. Invasion of the Data Snatchers, *Washington Post*, October 25.
Werts, C.E., Linn, R.L. and Joreskog, K.G. 1974. Interclass Reliability Estimates: Testing Structural Assumptions, *Education and Psychological Measurement,* 34, 25-33.

Appendix 1. Instrument Items

All items employed the 5 point Likert scale (Completely Disagree to Completely Agree), unless specified otherwise.

Construct	Item	Question
Behavioral Intention (BI)	BI1	I intend to periodically use anti-spyware applications to protect my computer from spyware.
	BI2	In the immediate future I intend to customize my browser and computer settings to prevent the intrusion of spyware to my computer.
	BI3	I intend to periodically check my browser and computer settings to prevent the intrusion of spyware to my computer.
Attitudes toward Behavior (AB)	AB1	For me, cleaning spyware from my computer would be: (Very bad idea – Very good idea)
	AB2	For me, preventing spyware from self-installing on my computer would be: (Very bad idea – Very good idea)
	AB3	For me, protecting my computer from spyware would be: (Very bad idea – Very good idea)
Subjective Norm (SN)	SN1	Most people who are important to me think it is a good idea to clean spyware from my computers.
	SN2	Most people who are important to me think it is a good idea to prevent spyware from running on my computer.
Perceived Behavioral Control (PBC)	PBC1	Please rate the difficulty for you to clean spyware from your computer using anti-spyware applications. (Extremely difficult – Extremely easy)
	PBC2	Please rate the difficulty for you to protect your computer from spyware. (Extremely difficult – Extremely easy)
Perceived Ease of Use (PEOU)	PEOU 1	The process of configuring my computer to protect from spyware is clear and understandable.
	PEOU 2	It would be easy for me to prevent spyware from running on my computer.
	PEOU 3	It would be easy for me to clean my computer from spyware.
Perceived Usefulness (PU)	PU1	I believe it is beneficial to protect my computer from spyware.
	PU2	I believe protecting from spyware will enhance my effectiveness in working with computer.
	PU3	I believe cleaning spyware off my computer will enhance my effectiveness in working with computer.
Awareness (TA)	TA1	I follow news and developments about the spyware technology.
	TA2	I discuss with friends and people around me security issues of Internet.
	TA3	I read about the problems of malicious software intruding Internet users' computers.
	TA4	I seek advice on computer web sites or magazines about anti-spyware products.
	TA5	I am aware of the spyware problems and consequences.
Control lability (C)	C1	I have the skill and resources to clean spyware from my computer.
	C2	I have the skill and resources to protect my computer from spyware.
	C3	Whether or not to clean spyware from my computer is completely under my control.
Self-Efficacy (SE)	SE1	I am confident that I can clean spyware off my system
	SE2	I am confident I can prevent unauthorized intrusion to my computer.
	SE3	I believe I can configure my computer to provide good protection from spyware.

About the Authors

Tamara Dinev is Assistant Professor in the Department of Information Technology and Operations Management (ITOM), Barry Kaye College of Business, Florida Atlantic University in Boca Raton, Florida. She received her Ph.D. in Theoretical Physics in 1997. Following several senior positions in IT companies, her interests migrated to MIS research and she joined the Florida Atlantic University ITOM faculty in 2000. Her research interests include Internet privacy and trust in online vendors, multicultural aspects of e-commerce use, spyware and negative technologies. She published in several journals including Information Systems Research, Communications of the ACM, International Journal of Electronic Commerce, European Journal of Information Systems, Journal of Global Information Management, e-Service Journal, and Behaviour and Information Technology. She received numerous Best Paper awards and nominations at major IS conferences.

Qing Hu is Professor of Information Systems in the Department of Information Technology & Operations Management, Barry Kaye College of Business, Florida Atlantic University in Boca Raton, Florida. He earned his Ph.D. in Computer Information Systems from the University of Miami, Florida, USA. His research interests include economics of information technology (IT), IT management strategies, and information security. His research work has been published in leading academic journals including MIS Quarterly, Information Systems Research, Communications of the ACM, California Management Review, Journal of Management Information Systems, IEEE Transactions on Software Engineering, Journal of Strategic Information Systems, and Communications of the AIS.

Journal of the Association for Information Systems
ISSN: 1536-9323

Editor
Kalle Lyytinen
Case Western Reserve University, USA