MIS Quarterly

SPECIAL ISSUE

PRACTICING SAFE COMPUTING: A MULTIMETHOD EMPIRICAL EXAMINATION OF HOME COMPUTER USER SECURITY BEHAVIORAL INTENTIONS[1]

By: **Catherine L. Anderson**
Decision, Operations, and Information Technologies Department
Robert H. Smith School of Business
University of Maryland
Van Munching Hall
College Park, MD 20742-1815
U.S.A.
Catherine_Anderson@rhsmith.umd.edu

Ritu Agarwal
Center for Health Information and Decision Systems
Robert H. Smith School of Business
University of Maryland
4327 Van Munching Hall
College Park, MD 20742-1815
U.S.A.
ragarwal@rhsmith.umd.edu

Abstract

Although firms are expending substantial resources to develop technology and processes that can help safeguard the security of their computing assets, increased attention is being focused on the role people play in maintaining a safe computing environment. Unlike employees in a work setting, home users are not subject to training, nor are they protected by a technical staff dedicated to keeping security software and hardware current. Thus, with over one billion people with access to the Internet, individual home computer users represent a significant point of weakness in achieving the security of the cyber infrastructure. We study the phenomenon of conscientious cybercitizens, defined as individuals who are motivated to take the necessary precautions under their direct control to secure their own computer and the Internet in a home setting. Using a multidisciplinary, phased approach, we develop a conceptual model of the conscientious cybercitizen. We present results from two studies—a survey and an experiment—conducted to understand the drivers of intentions to perform security-related behavior, and the interventions that can positively influence these drivers. In the first study, we use protection motivation theory as the underlying conceptual foundation and extend the theory by drawing upon the public goods literature and the concept of psychological ownership. Results from a survey of 594 home computer users from a wide range of demographic and socioeconomic backgrounds suggest that a home computer user's intention to perform security-related behavior is influenced by a combination of cognitive, social, and psychological components. In the second study, we draw upon the concepts of goal framing and self-view to examine how the proximal drivers of intentions to perform security-related behavior identified in the first study can be influenced by appropriate

[1]Detmar W. Straub was the accepting senior editor for this paper. Merrill Warkentin served as the associate editor.

Earlier versions of this paper were presented at 2005 Conference on Information Systems Technology and the 2006 International Conference on Information Systems. We gratefully acknowledge the feedback provided by the senior editor and the rest of the editorial team.

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

messaging. An experiment with 101 subjects is used to test the research hypotheses. Overall, the two studies shed important new light on creating more conscientious cybercitizens. Theoretical and practical implications of the findings are discussed.[2]

Keywords: Behavioral security, protection motivation, home computer user, goal framing, self-view, survey, experiment

Introduction

In late 2005, a watershed event occurred in the worldwide penetration of information and communication technology: the number of computer users with Internet access crossed the one billion mark (Gordon 2006). In recent times, of the global population of 1.3 billion users, at least 175 million are in the United States alone where, according to estimates by the U.S. Census Bureau, over half of all households own a home computer (Day et al. 2003). Access to the shared resources of the global network from homes and the interconnectedness it provides creates increased vulnerability as each home user represents a potential point of failure for security breaches such as the rapid proliferation of dangerous software via e-mail (Stanton and Stam 2006). As documented in the popular press, recovering from computer viruses and/or identity theft poses a significant financial and social cost (Borrus 2005; Campbell et al. 2003; Garg 2003; Krebs 2005). Indeed, home users were the most highly targeted sector in 2007, accounting for 95 percent of all attacks tracked by one of the leading security software and services vendors (Symantec 2009). To the extent that the online behavior and habits of these individuals can not only influence the security and privacy of their own personal data but can also potentially compromise the safety of the Internet infrastructure (Noyes 2007; Turner 2007), significant national attention is being focused on promoting individual behaviors that enhance computer and information security (Gross 2007; Walker 2007).

Within an organizational setting, security plans typically include initiatives to train employees in the appropriate use of technology and outline the required policies and procedures to be followed so as to mitigate risks in areas of vulnerability (e.g., NIH 2007). Unfortunately, individual home users are not required to have a security plan and, in fact, must take the initiative to educate themselves in the available security precautions. Acknowledging that individuals represent the weak link in security, recent research highlights the need for a socio-technical or behavioral approach to security (Sasse et al. 2001; Stanton et al. 2005; Workman et al. 2008). The behavior of the general public has ramifications that extend well beyond the home; other Internet users and organizations stand to suffer if the stability of the network becomes questionable due to security violations leading to a loss of confidence in conducting business and personal transactions over the Internet (Culnan et al. 2008; Symantec 2009). However, despite an acknowledgment of the importance of individual behavior and a recent interest in behavioral security research, there is limited understanding of what drives *home computer users* to behave in a secure manner online, and even less insight into how to influence their behavior.

Motivated by the fact that the security of the Internet is a highly consequential issue for individuals, organizations, and society, our broad research objective is to obtain a deeper understanding of the factors that influence a person's willingness to take the recommended security precautions under their direct control to protect their own computer and the Internet. We define security precautions to include individual actions such as running and consistently updating antivirus software, utilizing a firewall, being suspicious of e-mails from unknown sources, and effectively securing passwords. These four precautions form the foundation of the eight cyber security practices published by the National Cyber Security Alliance (NCSA 2007) and, particularly for the home user, are entirely voluntary.

We use a multimethod phased approach with two distinct studies designed to provide a detailed understanding of individual intentions to engage in security-related behavior (Mingers 2001). The phased approach further enables us to balance rigor and relevance in our investigations (Benbasat and Zmud 1999; Rosemann and Vessey 2008; Senn 1998).[3] Although we assess intentions rather than behavior due to difficulties associated with observing actual security behavior (Vroom and von Solms 2004), nevertheless, the relationship between intentions and actual behavior has been shown to be strong and consistent (Sheeran 2002; Venkatesh et al. 2003; Webb and Sheeran 2006), as well as theoretically grounded (Ajzen 1991; Fishbein and Ajzen 1975). Thus, even though the study technically measures intentions, it is substantively about behavior. As a result, we refer to security behavior throughout the paper except when explicitly referring to the operationalization of the variable. We pose three research questions:

[2]Editor's Note: *MIS Quarterly* has, as part of its mission, a charge to understand the management of computing in domains larger than organizations. Specifically, as stated in 2009, the mission stresses the "societal implications" of use of IT resources.

[3]A more detailed discussion of our multimethod approach is available in Appendix H.

1. What are the factors influencing a home computer user's security behavior?

2. Are there differences in the factors influencing a home computer user's intentions to protect her own computer versus the Internet?

3. Can the strength of some of these factors be changed through message cues?

Study 1 addresses the first two research questions. Here we synthesize relevant theory from three disciplines (marketing, economics, and psychology) to develop a comprehensive model describing the antecedents of individuals' intentions to practice safe computing at home. We test this using a field study approach with data gathered via a survey from a broad sample of 594 users and identify the influential drivers of individuals' intentions to take security precautions. Next, in study 2, we use the empirical findings from the survey along with theory from marketing and psychology in an experimental setting to understand how these proximal drivers of security behavior can be proactively manipulated, thereby addressing the third research question.[4]

Protection motivation theory (PMT), which predicts individual response when faced with a threat, provides the core theoretical foundation for study 1. Although others have applied PMT to the security context (Johnston and Warkentin 2010; Rifon et al. 2005; Woon et al. 2005; Workman et al. 2008), we extend extant work in three important ways. First, from a theoretical perspective, these studies have limited their focus primarily to the constructs of PMT, thereby ignoring other determinants of behavior that may be important. To the degree that the Internet infrastructure is a non-rival (i.e., the Internet can be "consumed" or utilized by multiple consumers simultaneously) and non-excludable (i.e., it is not possible to prohibit people from enjoying the benefits of the Internet) public good, the economics literature on individual behavior in the context of public goods is arguably relevant here, as it provides insight into the motivations of an individual to take essentially voluntary steps to protect a shared network. Public goods theory suggests that people will cooperate in public good situations, depending on the perceived contributions of others; thus we extend PMT to include this concept of descriptive norm. Further, the majority of past work on PMT is in the context of health risks to the self (e.g., Ho 1998, Pechmann et al. 2003, Rippetoe and Rogers 1983). Therefore, we incorporate consideration for factors relevant in the security context, given that the threats are to an object and not the self directly. Theory in psychology and organizational behavior draws attention to the notion of psychological ownership or the "connection" that individuals feel toward objects and concepts. We extend the core PMT and theorize that this construct is relevant to home security behavior because individuals may perceive different levels of ownership toward the resource they are intending to protect.

Second, prior studies with PMT have either been exploratory in nature (Rifon et al. 2005) or investigated the drivers of intentions to use specific precautions such as a firewall, operationalizing security usage as a binary variable (Woon et al. 2005), or have focused on employees (Johnston and Warkentin 2010; Workman et al. 2008). In contrast, our study focuses on home computer users and distinguishes between intentions to secure one's own computer from intentions to secure the Internet, and utilizes a nuanced operational measure for each outcome. Finally, we are able to test the extended model using a rich data set of close to 600 respondents representing a wide range of demographic profiles, thereby providing robust empirical evidence for the posited relationships. Study 1 reveals that psychological ownership, attitudes toward security-related behavior, and subjective and descriptive norm collectively influence security behavior toward one's own computer and toward the Internet.

Study 1 serves as input for the next phase of our sequential research process (Mingers 2001). In study 2, we seek the most effective mix of message characteristics that influence these variables positively. We draw on theory from marketing and psychology (Higgins 1997; Lee et al. 2000) to argue that two aspects of messages regarding security are germane: those that focus individuals' self-view toward *independence*, and those that emphasize the positive outcomes associated with a behavior in contrast to the negative outcomes associated with not performing it. We report findings from an experiment with 101 subjects where we manipulated message framing and self-view and examined their effects on attitudes, and subjective and descriptive norms in the context of security behaviors. Collectively, the two studies provide new and important insights into the mechanisms underlying individuals' security behaviors at home and how they can be positively influenced to create more conscientious cybercitizens. They offer guidance on specific messages and mechanisms to increase individuals' propensity to practice safe computing.

The rest of the paper proceeds as follows. We begin with study 1, where we describe our individual security motivation model and develop seven research hypotheses related to understanding the drivers of home user security behavior. This is followed by the results of study 1, including a discussion of the findings. Next, we turn to study 2, which

[4]The rationale underlying the design of the two studies is available in Appendix H.

builds on the findings of study 1 to provide a richer understanding of the security phenomenon and enables more concrete recommendations for practice. Finally, we discuss the implications of the two studies collectively as well as the overall research process.

Background Literature

The extant information systems literature on security does not fully consider the ramifications of one's protective security behavior in response to a threatened object or possession that is separate from one's self. However, a robust body of theoretically based security research has recently developed and provides insight into our domain of interest. We briefly review key findings from this stream of research first, followed by the relevant literature from marketing, economics, and psychology on topics relevant to understanding how one may respond to security threats to possessions and other important objects.

Security Literature

Information systems security has been addressed from multiple perspectives, including the technical design of security mechanisms and more socio-technical treatments of the topic. We focus our review on research that examines the behavioral aspect of security, as this work is most relevant to our research. Table 1 summarizes research in the behavioral security domain, including studies conducted in the work context first followed by studies conducted in non-work settings. As can be seen, the majority of research addressing the human side of the security issue has been conducted within organizations, with a goal of understanding employee security behavior (e.g., Boss et al. 2009; D'Arcy et al. 2009; Herath and Rao 2009; Myyry et al. 2009; Pahnila et al. 2007; Stanton et al. 2005; Workman et al. 2008); however, recent attention has been given to the home user (e.g., LaRose et al. 2008; Woon et al. 2005).

A number of studies conducted with both employees and home users suggest that preventive behaviors are influenced by two processes, called *threat appraisal* and *coping appraisal*, which are key tenets of the protection motivation yheory (PMT). An individual who is aware of security threats forms beliefs about the perceived severity and probability of the threat, which are then evaluated against the beliefs formed about the efficacy of potential response. Several studies show that threat appraisal and coping response variables influence security behavior in the workplace (Johnston and Warkentin 2010; Lee and Larsen 2009; Workman et al. 2008) and at home (LaRose et al. 2008; Woon et al. 2005). However, while Pahnila et al. (2007) found support for the influence of threat appraisal on attitude toward complying with security policy, they did not find support for the influence of coping appraisal on attitude. Pahnila et al. incorporate a variety of factors in addition to those of PMT such as sanctions, rewards, and facilitating conditions. The significance of these variables suggests that although PMT may have explanatory power for user security behavior, there are likely to be other important factors influencing security behavior. In addition to the coping and threat appraisal processes, an individual's level of self-efficacy influences security behavior (LaRose et al. 2008; Lee and Larsen 2009; Woon et al. 2005; Workman et al. 2008), as does the extent to which she believes it is her responsibility to take control of security (Workman et al. 2008).

Although theoretically based research in behavioral security has increased, less attention has been paid to social factors, even though the information systems adoption literature and the underlying theories they draw upon suggests (e.g., Brown and Venkatesh 2005; Venkatesh and Davis 2000) that norms can be influential in the formation of behavior. The few studies that have included social factors have yielded mixed results. For example, Pahnila et al. find that subjective norm has a significant effect on intentions to comply with security policy in a workplace setting and Lee and Larsen (2009) find that social influence is significant for IT-intensive industry and expert groups but not for non-IT-intensive and non-IS expert groups. Lee and Kozar (2005) find no such relationship between norms and intentions to adopt anti-spyware software in a home setting. These conflicting findings may be reflective of the mandatory versus voluntary nature of security behavior at work versus at home (Venkatesh and Davis 2000). However, Lee and Kozar find support for other social influences such as the visibility of anti-spyware use by others, and perceptions of how anti-spyware use may improve one's image. In general, household decisions are susceptible to normative influences (Burnkrant and Cousineau 1975) which, when combined with the discrepant findings between social influences in the home versus work contexts, suggest the need for further research to explore the potential role of norms in the context of home user security behavior.

Workplace studies point to the potential of security policies and related rewards and sanctions for influencing security behavior (Boss et al. 2009; Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009; Myyry et al. 2009; Pahnila et al. 2007; Siponen and Vance 2010; Straub 1990). Although these factors are less relevant for home users because they are not subject to mandatory training efforts, nor are they likely to be monitored in terms of their security behavior in their own homes, nevertheless, other factors unique to the work-

place can provide insight into potential variables of interest in understanding what motivates home users. For example, several studies conducted in a work environment, which are more conceptual and qualitative in nature, recommend fostering a security culture by building the employees' psychological contract with the organization (Leach 2003), and indicate that employees with more allegiance to the organization tend to exhibit increased compliance with security policies (Sasse et al. 2001). These findings suggest that individuals are likely to be influenced by how closely they feel tied to the object or objects they are asked to, or volitionally seek to, protect with preventive measures.

A recurrent theme in the literature is that while an awareness of threats and appropriate response is necessary to increase security behavior, it is not sufficient (Dodge et al. 2007; Furnell et al. 2007; Lee and Kozar 2005; Rhee et al 2005; Stanton et al. 2005; Vroom and von Solms 2004; Weirich and Sasse 2001). Thus, it is important to identify the drivers of security behavior in different settings particularly since inconsistent findings are common, as indicated above. In this study, we expand our thinking about security behavior based on the notion that individuals are protecting something separate from themselves, and compare influencing factors motivating intentions to protect one's own computer versus the Internet.

Protection Motivation Literature

Protection mtivation teory (PMT) has formed the basis for prior security research (e.g., Johnston and Warkentin 2010; Lee and Larsen 2009; Pahnila et al. 2007; Woon et al. 2005; Workman et al. 2008) and provides the core foundation for our model. We briefly describe this literature, which provides a nuanced theoretical explanation for why people engage in potentially harmful behaviors.[5] PMT, proposed by Rogers (1975), was originally based on expectancy-value theories and identified the cognitive processes an individual experiences when faced with a threat. The base protection motivation model theorizes that a person assesses a threat based on their own perception of the severity of the threat, susceptibility to the threat, and its probability of occurrence. Once the threat has been evaluated, the person assesses the efficacy of the recommended response to the threat and self-efficacy regarding the protective actions required to mitigate the threat. As described in a meta analysis conducted by Floyd et al. (2000), PMT is one of the most powerful explanatory theories predicting individual *intentions* to take protective actions. PMT is consistent with Lazarus' (1991) primary and secondary appraisal process. Lazarus argues that an individual first becomes aware of situational facts and then evaluates these facts as they relate to personal perception of the environment. The primary appraisal process involves a determination regarding the personal relevance of the facts, and relates to the threat assessment process in the protection motivation model. The secondary appraisal process involves an assessment of one's resources for coping with a situation, and is represented in protection motivation theory by the perceived efficacy of the proposed response and self-efficacy. In general, home computer users demonstrate an understanding of common security terms and indicate relatively high usage of commonly recommended security precautions such as the ones on which we focus in this study. For example, in a study conducted in the United Kingdom, 99 percent of respondents indicated an understanding of the terms *computer virus* and *hacker* (Furnell et al. 2007). The vast majority of these same respondents indicated an understanding of the terms *firewall*, *spyware* and *identity theft* (96 percent, 89 percent, and 92 percent, respectively). Michigan State University's Internet Safety Survey (Schulman, Ronca, & Bucuvalas, Inc. 2007) indicates that 77 percent of home users utilize antivirus software, 82 percent of users with a wireless network at home use a firewall, and 75 percent exercise care when opening e-mail attachments. Collectively, these findings provide evidence that home computer users have sufficient knowledge to begin threat assessment and coping assessment processes regarding security behavior.

Theories of social behavior note that individual action is circumscribed within a social context (Ajzen 1988). Tanner et al. (1991) revised PMT to incorporate the impact of social norms and prior experience on the protection motivation process. For example, teenagers may believe smoking is bad for their health but may smoke due to a social pressure to be accepted. Although the use of security precautions in a home environment may not immediately suggest a concern for social pressure, nonetheless some aspects of social influence, particularly those in the form of censure or embarrassment, are relevant. For instance, if an individual finds he/she has spread a virus unknowingly to friends via e-mail, he/she may lose some social standing. In fact, one of the factors found to foster positive password security behavior in employees is the potential threat of embarrassment (Weirich and Sasse 2001). Tanner et al.'s revision of PMT also incorporates an individual's prior experience, which contributes to perceptions about costs and benefits associated with actions, as influencing behavior (Bulgurcu et al. 2010; Herath and Rao 2009; Lee and Larsen 2009; Johnston and Warkentin 2010; Workman et al. 2008.)

PMT has largely been applied in health and environmental settings to determine which advertising messages effectively

[5]For further information regarding protection motivation theory research, see Floyd et al. (2000).

Table 1. Summary of Behavioral Security Literature (In Reverse Chronological Order by Work/Non-Work Settings)

Author (Date)	User Base/Context	Methodology	Description	Theory Applied
Workplace Settings				
Bulgurcu et al. (2010)	Employees/ Multiple Organizations	Field study: data collected via surveys	Findings suggest that employee intention to comply with information security policy is influenced by attitude, normative beliefs, and self-efficacy to comply. Employee attitude is influenced by benefit of compliance, and costs associated with both compliance and non-compliance which are beliefs about overall consequences of compliance/non-compliance. Information security awareness positively influences attitude and outcome beliefs.	Theory of Planned Behavior, Rational Choice Theory
Johnston and Warkentin (2010)	Faculty, staff and students at a large university	Experiment	Investigates the influence of fear appeals on end-user compliance with computer security recommendations. Results suggest fear appeals influence end-user behavioral intentions but not uniformly. Perceptions of self-efficacy, response efficacy, threat severity, and social influence also play a role.	Fear Appeal Theory, Protection Motivation Theory
Siponen and Vance (2010)	Employees/ Multiple Organizations	Field study: data collected via surveys	Results suggest that neutralization theory provides an explanation for IS security policy violations. When neutralization is incororated in the model, no effects of general deterrence theory are significant.	Neutralization Theory, General Deterrence Theory
Boss et al. (2009)	Employees/ Organization (1)	Field study: data collected via surveys	Using organizational control as a lens, a model is built to explain security precaution-taking behavior. Results find that specifying policies and evaluating behaviors influences the perceived mandatoriness of security policies. Mandatoriness effectively motivates individuals to take security precautions.	Control Theory
D'Arcy et al. (2009)	Employees/ Multiple Organizations	Field study: data collected via surveys	Extends general deterrence theory by examining security countermeasures (security policies, SETA program, computer monitoring) as antecedents to perceived certainty and severity of sanctions. Findings suggest that all three countermeasures deter IS misuse intentions. Perceived severity of sanctions (as opposed to certainty of sanctions) is most effective at deterring IS misuse.	General Deterrence Theory
Herath and Rao (2009)	Employees/ Multiple Organizations	Field study: data collected via surveys	Findings suggest that organizational commitment and social influence increase compliance intentions. Policy attitudes influenced by severity of breaches, response efficacy, self-efficacy and response costs. Employees underestimate probability of security breaches.	Decomposed Theory of Planned Behavior, Protection Motivation Theory, General Deterrence Theory
Lee and Larsen (2009)	Employees/ Multiple Organizations	Field study: data collected via surveys	Threat and coping appraisal were found to predict adoption intentions of anti-malware software by small- and medium-sized business executives. Vendor support facilitated adoption for IS experts/IT intensive industry while IT budget facilitated adoption for non-IS experts/non-IT intensive industry groups.	Protection Motivation Theory expanded to include social influence and situation-specific control factors
Myyry et al. (2009)	Employees in 1 organization and part-time graduate students	Field study: data collected via surveys	Applies concepts from moral reasoning and values to understand compliance with IS security policies. Preconventional moral reasoning, which focuses on fear of sanctions, had a positive influence on both hypothetical and actual compliance. Openness to change and conventional moral reasoning were negatively associated with compliance behavior.	Theory of Cognitive Moral Development,Theory of Motivational Types of Values
Workman et al. (2008)	588 Employees/ Organization (1)	Field study: data collected via surveys and secondary data	Proposes and tests a threat control model to explain why users who know how to protect their systems fail to do so. Findings suggest threat assessment and coping assessment influence subjective and objective omissive behavior. Self-efficacy and locus of control drawn from social cognitive theory affect omissive behaviors.	Protection Motivation Theory, Social Cognitive Theory

Table 1. Summary of Behavioral Security Literature (In Reverse Chronological Order by Work/Non-Work Settings) (Continued)

Author (Date)	User Base/Context	Methodology	Description	Theory Applied
Pahnila et al. (2007)	245 Employees/ Organization (1)	Field study: data collected via surveys	Proposes and tests a theoretical model explaining employees' IS security policy compliance. Employees' attitude, normative beliefs and habits have significant effect on intentions to comply with security policy. Threat appraisal and facilitating conditions impact attitude but coping appraisal does not. Sanctions do not influence intentions to comply. Rewards did not influence actual compliance.	General Deterrence Theory, Protection Motivation Theory, Theory of Reasoned Action, Information Systems Success and Triandis' Behavioral Framework and Rewards
Dodge et al. (2007)	Employee/ Organization	Experiment	Describes the process involved in establishing and implementing an evaluation of one aspect of user education involving phishing.	N/A
Stanton et al. (2005)	1,167 Employees/ Organizations (various within the U.S.)	Field study: data collected via surveys	Created a taxonomy of end user security-related behavior along two dimensions: level of technical knowledge required and intentionality of behavior. Tested taxonomy via a survey to identify six categories of end users. Evidence that good password behavior is related to training, awareness, monitoring and motivation.	N/A
Vroom and von Solms (2004)	Organization level	Conceptual	Argues that auditing employee security behavior is difficult. Proposes an alternative to auditing which is to create a more information security conscious organizational culture.	Schien's 3-level model of organizational culture
Leach (2003)	Employee / Organization	Conceptual	Suggests strengthening the employees' psychological contract with the organization in order to reduce the internal security threat.	N/A
Weirich and Sasse (2001)	17 Employees/ students	Field study: data collected via interviews	Findings identify several mechanisms that undermine security conscious behavior such as low probability of attack, severity of consequences of attack are minimal, and low response efficacy. Individuals performing in a more security conscious manner did so to avoid embarrassment or because of allegiance to the organization, prior experience with break-ins or to maintain privacy. Social marketing techniques are suggested to associate positive qualities with proper behavior and negative qualities with bad behavior.	N/A
Sasse et al. (2001)	Employees / Organization (1)	Field study: data collected via mixed methods (surveys, secondary data, interviews)	Presented examples of how undesirable user behavior with passwords can be caused by poorly designed and implemented procedures that conflict with task demands and are inconsistent with characteristics of human memory. Findings also suggest the importance of motivation and training to address 7 issues that lead to undesirable password behavior including low probability and severity of threat, low perceived response efficacy and social issues such as trust vs. paranoia. Findings seem to suggest that employees who feel a stronger sense of organizational commitment are more careful with their password behavior.	N/A
Straub (1990)	Employees / Multiple Organizations	Field study: data collected via surveys	Findings suggest deterrence measures such as policies and guidelines about appropriate system use and penalties are effective at improving security while other alternative explanations such as motivational and environmental factors were found to be insignificant.	General deterrence theory

Table 1. Summary of Behavioral Security Literature (In Reverse Chronological Order by Work/Non-Work Settings) (Continued)

Author (Date)	User Base/Context	Methodology	Description	Theory Applied
Non-Work Settings				
LaRose et al. (2008)	206 Students	Experiment	Findings suggest the possibility of improving safety behavior by emphasizing the user's personal responsibility in a message. However, it depends on the user's involvement and level of self-efficacy. Personal responsibility, self-efficacy and response efficacy were most related to intentions to engage in safe online behavior.	Protection Motivation Theory, Elaboration Likelihood Model (involvement), Social Cognitive Theory (self-regulation)
Furnell et al. (2007)	415 home users	Field study: data collected via surveys	Assesses perceptions of security issues and attitudes toward use of related safeguards. Claimed understanding of common security terms and reported usage of common safeguards was very high. However, questions to assess user understanding of concepts and actual role of safeguards was not convincing.	N/A
Lee and Kozar (2005)	212 Internet Users	Field study: data collected via surveys	Findings suggest that attitude (relative advantage and moral compatibility), social influence (visibility of others' use and image) and perceived behavioral control (computing capacity and trialability) influence intentions to adopt anti-spyware software.	TPB, IT innovation
Rhee et al. (2005)	248 working Master's students	Field study: data collected via surveys	Finds that users demonstrate an optimistic bias with regard to security risk. Individuals perceive their information security threat as lower than a friend's risk and the bias increases further when comparing the risk to an average other. Perceived controllability decreases an individual's perception of information security self-risk.	Social Comparison Theory, Optimistic Bias
Woon et al. (2005)	189 Home Users	Field study: data collected via surveys	Perceived severity, response efficacy, self efficacy and response cost found to be predictors of security behavior in the context of home wireless network usage. Dichotomous DV (have enabled/ have not enabled a firewall on home wireless network).	Protection Motivation Theory

motivate a person to take action when faced with a threat (for examples in health-related anti-smoking settings, see Ho (1998) and Pechmann et al. (2003); for environmental areas of concern such as energy and water conservation, see Obermiller (1995)). The cybersecurity issue is similar to select environmental and health concerns in that every individual can make a difference. Securing cyberspace is defined in "National Strategy to Secure Cyberspace" (DHS 2003) as preserving the healthy functioning of the infrastructure that supports critical work. It relies, in part, on every citizen doing his/her share to ensure security. Thus, individuals must not only believe that individual action is essential in the fight to secure cyberspace, they must further perceive that individual action makes a *difference* in the security and privacy of personal information.

In his extension of PMT to an advertising effects model, Obermiller (1995) introduces concern, determined by severity and probability of threat, and perceived consumer effectiveness, determined by self-efficacy and response efficacy. Concern and perceived consumer effectiveness, in turn, influence consumer attitude. He finds that advertising messages should vary based on whether or not the public's concern level regarding the threat is already high or is low. If concern is high, advertising messages should focus on bolstering perceived consumer effectiveness by affirming the impact of individual action with regard to the desired threat response. If concern is low, advertising messages should focus on building the general concern level. In the instance of cybersecurity, organizations seeking to persuade citizens to adopt security precautions need to have an understanding of individual's predispositions in order to appropriately tailor training and awareness initiatives, which makes marketing studies such as Obermiller's particularly relevant.

Public Goods Research

The economics literature, which examines consumer behavior in public goods situations, also has relevance to the home user security behavior issue. The Internet is not a public good relying on monetary contributions by individuals for its

survival, like public television or various charitable organizations. However, it is a non-excludable resource in that the public can access it only by paying the cost of Internet service provision. Pleas to the public to take steps to secure cyberspace are analogous to requests for voluntary contributions of time and effort to secure the stability of the publicly shared Internet. Much research has been conducted to determine what factors influence an individual's willingness to contribute to public goods. (Frey and Meier 2004; Keser and van Winden 2000; van Dijk and Wilke 1997). This literature identifies a tendency for people to *conditionally* cooperate in public goods situations, where the cooperation is dependent upon the perceived contributions of others. For instance, Frey and Meier (2004) report a significant correlation between expectations of others to contribute and an individual's own contribution. For the purposes of this study, a descriptive social norm such as what an individual believes most other people do to address security is likely to exhibit an influence on individual intentions to protect the Internet.

Descriptive norms also influence individuals' intentions in nonpublic domain situations (Astrom and Rise 2001; Conner and McMillan, 1999; Rivis and Sheeran 2003b), suggesting that such norms may be particularly relevant in predicting intentions to perform security-related behaviors to protect one's own computer. In a study conducted on anti-spyware software adoption, visibility of others' use of the software influenced intentions to adopt the software (Lee and Kozar 2005). Observing others' use of software is similar to the concept of descriptive norm in that if I see others doing it, I will be more inclined to do it myself. Thus, it is important to explore the potential influence of this social norm on security behavior toward the Internet and one's own computer.

Psychological Ownership

The final stream of research relevant to a study of home computer user security behavior is in the psychology and organizational behavior discipline and involves the psychological aspects of *ownership*. People experience connections to various targets of possession, including objects such as cars and homes (Dittmar 1992). A sense of ownership can also be experienced in regard to nonphysical targets such as ideas, creative endeavors, and other people (Isaacs 1933). To the extent that security behavior is enacted to protect entities other than oneself (such as computers, data, and the Internet), this stream of literature provides important insight into understanding the factors driving security behavior.

Psychological ownership generally refers to a state in which an individual feels as though the target is "theirs" (Pierce et al. 2003). The sense of ownership individuals come to feel for various entities is generated from a combination of biological need and social experiences (Dittmar 1992; Pierce et al. 2003). Most relevant to the security context are two human motives for psychological ownership: efficacy/effectance and self-identity.

One functional need served by possessions is to make possible desired outcomes in an individual's environment (Furby 1978; White 1959). In this manner, possessions enable or effect activities and pleasures serving an effectance motivation (Dittmar 1992; Furby 1978; Pierce et al. 2003; White 1959). The need to experience causal efficacy can lead to psychological ownership of a variety of entities that can even come to be considered as part of the extended self (Furby 1978). The importance and need for enacting such influences on one's environment likely varies from one individual to the next. In the home computer use context, an individual's computer and the Internet enable a variety of activities which the individual may value, such as entertainment, communication, and economic transactions. Thus, the individual experiences a sense of psychological ownership for the computer and Internet because these two "objects" facilitate activities the individual finds positive and desirable.

A second need served by possessions is as an expression of self-identity (Pierce et al. 2003). Through interaction with and public display of possessions, individuals express attitudes and values and communicate who they are and what they do (Dittmar 1992; Levy 1959). One example involves individuals expressing their concern for the environment by driving hybrid vehicles that use alternative forms of energy for fuel (Heffner et al. 2005). Personal computers have also become expressions of uniqueness as computer companies allow customization of laptop covers, enabling users to convey individuality by distinguishing the appearance of their laptop. It has also been suggested that possessions play a significant part in social interaction (Dittmar 1992). The Internet and one's personal computer serve as a gateway to forms of technology-mediated communication such as online communities, social networking websites, and e-mail. Therefore, people form strong psychological attachments to objects, which provide them with a sense of self and that facilitate social interaction (Dittmar 1992; Pierce et al. 2003). Effects of psychological ownership include feelings of responsibility and, as a consequence, the individual will proactively take action to protect, care for, and nurture targets to which her sense of self is closely tied (Dipboye 1977; Korman 1970). Therefore, in the context of our study, we expect individuals who feel a strong sense of psychological ownership for their own computer or for the Internet to have stronger intentions to take appropriate preventive security measures to secure the focal objects.

In summary, no single stream of literature completely frames the home computer user security behavior phenomenon;

however, each of the literatures reviewed above provides useful insights. We synthesize this literature and its resulting key constructs to derive an overall conceptualization of the drivers of security behavior.

A Causal Model of the Conscientious Cybercitizen

The core of the conceptual model underlying our study, shown in Figure 1, is drawn primarily from Tanner et al.'s (1991) extended version of protection motivation theory which incorporates aspects of social norm. We further extend PMT by including the additional constructs of descriptive norm, drawn from public goods research, and psychological ownership from the psychology and organizational behavior literature.

We examine two distinct outcomes: behavioral intentions to secure one's own computer and behavioral intentions to secure the Internet. These intentions are theorized to be driven by three key determinants: attitudes toward security-related behavior, social influence in the form of subjective and descriptive norm, and psychological ownership of the relevant object. We note that the overall structure of the model is also consistent with the theory of planned behavior (TPB) (Ajzen 1991) and the theory of reasoned action (TRA) (Fishbein and Ajzen 1975) from social psychology. Indeed, as observed by Floyd et al. (2000), the theories used to explain the initiation of protective behaviors, including TRA, exhibit more similarities than differences.

Explaining Attitude Toward Security-Related Behavior

We theorize that attitude toward security-related behavior—the extent to which the individual believes that taking security precautions is a desirable action—is collectively determined by concerns regarding security threats, perceived citizen effectiveness, and self-efficacy related to security behavior. We define this construct consistent with the dominant conceptualization of attitude in the psychology literature as an overall feeling of liking or disliking a particular behavior (Ajzen 1988; Ajzen and Fishbein 1980).

A key tenet of PMT is that the individual must feel a level of concern related to the potential threat (Rogers 1975). For instance, if an individual believes that smoking causes no harm, the necessary affect toward protecting oneself against the negative consequences of smoking is not likely to be activated. Concern represents the threat appraisal aspect of PMT, which has been related to home firewall behavior (Woon et al. 2005), security behavior (Lee and Larsen 2009; Workman et al. 2008), and security compliance attitude (Pahnila et al. 2007). The greater and more relevant the threat appears to be, the more likely the individual is to have a positive attitude about taking action (Lee and Larsen 2009; Liang and Xue 2009; Pahnila et al. 2007; Witte 1992; Woon et al. 2005). This positive attitude results in stronger intentions to act (Rogers 1975) and a lower likelihood that the individual will ignore security behavior (Workman et al. 2008). Thus, we hypothesize

H1: Concern regarding security threats is positively related to attitude toward security-related behavior.

Feeling concerned about an issue is distinct from feeling as if one can make a difference with regard to an issue by taking a particular individual action. In the context of this study, individuals may be concerned about security and associated threats, but may believe that nothing much can be done to mitigate or eliminate such threats (Obermiller 1995). In order for individuals to perceive themselves as playing an effective role in minimizing security threats, they must perceive that the recommended coping response is potentially effective. As a result, we expect perceived citizen effectiveness and self-efficacy to be significant factors influencing attitude toward security-related behavior. Perceived citizen effectiveness is conceptually similar to Obermiller's (1995) perceived consumer effectiveness, and represents an individual's belief that his/her individual actions can make a difference in a particular situation. Perceptions regarding the efficacy of the coping response come from PMT (Rogers 1975; Tanner et al. 1991), and are consistent with Lazarus' (1991) secondary coping appraisal process. Security studies suggest that individuals with a higher perception of response efficacy are less likely to omit security behavior in the workplace (Bulgurcu et al. 2010; Lee and Larsen 2009; Workman et al. 2008) and are more likely to use a firewall on their home wireless network (Woon et al. 2005). If an individual believes the available security precautions are effective in securing cyberspace, he/she is more likely to believe that individual action can make a difference. Therefore, we expect

H2: Perceived citizen effectiveness is positively related to attitude toward security-related behavior.

In a similar spirit, the individual must believe that he/she can perform the necessary response as required. As reviewed earlier, self-efficacy is incorporated in extensions to the PMT (Arthur and Quester 2004; Tanner et al. 1991). It is also a key construct in models of IT use behavior (e.g., Lewis et al. 2003; Pavlou and Fygenson 2006; Taylor and Todd 1995). Its

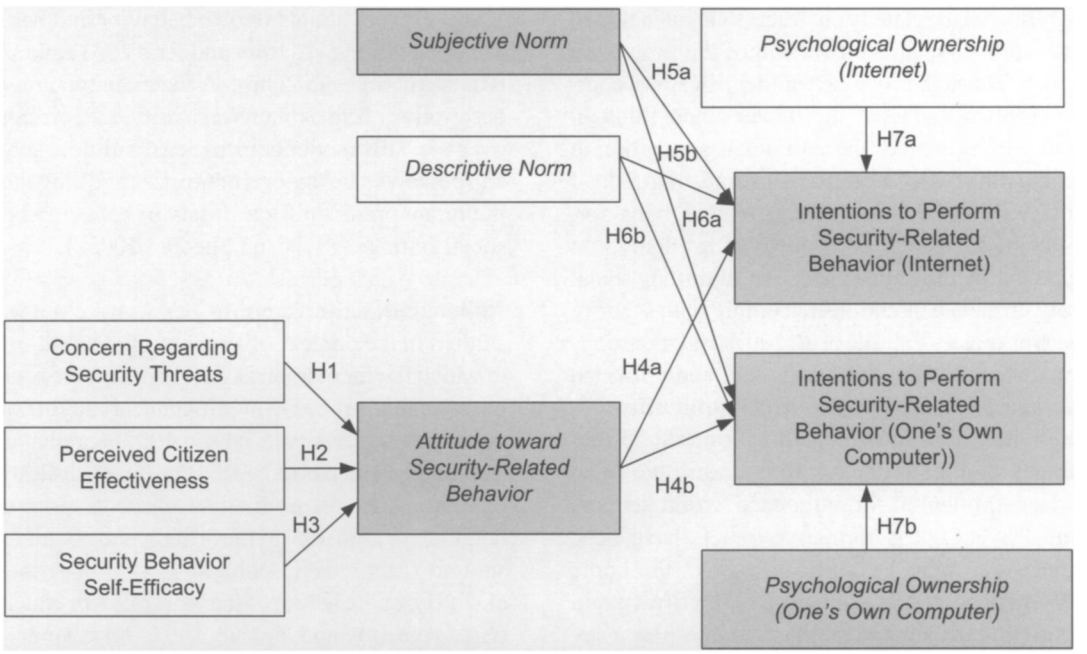

Figure 1. Individual Security Motivation Model

inclusion as a predictor of attitude is further consistent with Lazarus' secondary coping appraisal process. Moreover, self efficacy influences security behavior (Herath and Rao 2009; LaRose et al. 2008; Woon et al. 2005; Workman et al. 2008). The individual's belief in his/her own ability to take the recommended precautions is expected to contribute directly to activating the necessary affect toward taking security precautions.

H3: Security behavior self-efficacy is positively related to attitude toward security-related behavior.

Explaining Intentions to Perform Security-Related Behavior

We distinguish between behavioral intentions to protect one's computer and protecting the Internet. Although we acknowledge that the two intentions are likely to be highly related,[6] we argue that it is theoretically important to discriminate the two constructs. While the former is reflective of an action that has only personal consequences (i.e., placing the individual at risk), the latter has far more wide-reaching impacts (e.g., propagating a virus on the Internet.) To draw an analogy, when an individual washes her hands, she is likely primarily doing so with the intention of protecting herself from getting sick from germs passed through surface-to-surface contact. However, she also is partly intending to stop the spread of her own germs to others if she has a cold or virus and, thus, has an intention that reaches beyond her own more egocentric needs and creates an outcome that benefits the public at large. To the extent that the salient referent is distinct in each case, it is possible that the motivations that drive these two related intentions may be different.

The relationship between attitude and behavioral intentions has been theorized and extensively tested in a robust body of literature from multiple disciplines (Armitage and Conner 2001; Sheeran and Taylor 1997; Venkatesh et al. 2003). Attitudes toward specific behaviors influence intentions to perform the behavior because individuals seek cognitive consonance between feelings and actions (Ajzen and Fishbein 1980). Therefore, we test

H4a: Attitude toward security-related behavior is positively related to behavioral intentions to protect the Internet.

H4b: Attitude toward security-related behavior is positively related to behavioral intentions to protect one's own computer.

[6]To account for this, we include a path from intentions to protect one's own computer to intentions to protect the Internet in the empirical test of our model.

In addition to attitude, security behavior encompasses a social component, as reflected in related constructs that are included in Tanner et al.'s (1991) expanded version of the protection motivation model. Through processes of identification, compliance, and internalization, what significant others think an individual should do influences the individual's intention to perform the behavior. Sasse et al. (2001) find that risk of embarrassment plays a role in security-related behavior, further underscoring the social component of influences on individual behavior in the workplace. In addition, social norms positively influence intentions to comply with security behavior in the workplace (Pahnila et al. 2007) and intentions to adopt anti-malware software by small- and medium-sized businesses (Lee and Larsen 2009). While taking security precautions in one's home is not mandated as it might be in a work environment, and although subjective norm has been found to be less influential in voluntary work settings (Venkatesh and Davis 2000), normative beliefs have been shown, nonetheless, to play a significant role in the home environment (Burnkrant and Cousineau 1975). Brown and Venkatesh (2005) find friends and family members play a key role in the adoption of PCs in homes. Therefore, we expect the opinions of important others to play a role in the determination of behavioral intentions.

H5a: Subjective norm is positively related to behavioral intentions to protect the Internet.

H5b: Subjective norm is positively related to behavioral intentions to protect one's own computer.

As noted before, a unique aspect of the Internet is that it is a public good that can be consumed even by individuals who do not have to pay directly for its establishment and maintenance. As the economics literature suggests, people tend to conditionally cooperate in public goods situations, dependent upon the perceived contributions of others. Descriptive norm, defined as the extent to which one believes others are performing the behavior, taps into the propensity an individual may have to indirectly reciprocate the believed behavior of others (Frey and Meier 2004; Keser and van Winden 2000; van Dijk and Wilke 1997). For the purposes of this study, the relevant descriptive norm is what an individual believes most other people do to address security, and is posited to influence an individual's intentions to perform preventive behaviors to protect the Internet. Therefore, we test

H6a: Descriptive norm is positively related to behavioral intentions to protect the Internet.

The influence of descriptive norm is not confined to public goods literature (Astrom and Rise 2001; Conner and McMillan, 1999; Rivis and Sheeran 2003b). The actions of others can provide essential information as an individual makes choices about her own behavior in other settings, such as healthy eating (Astrom and Rise 2001) and binge drinking (Rivis and Sheeran 2006). A meta-analytic review finds that descriptive norm explains an additional 5 percent of variance over the TPB model constructs of attitude, subjective norm, and perceived behavioral control, suggesting that it may be an important predictor for a variety of behavioral phenomena in social settings (Rivis and Sheeran 2003a).

Although descriptive norms *per se* have not been explicitly studied in the context of IS research, visibility, or the degree to which the innovation is visible within the organization, has been found to be a significant predictor of technology adoption (Agarwal and Prasad 1997; Karahanna et al. 1999; Moore and Benbasat 1991; Plouffe et al. 2001). While its operationalization normally reflects a more objective and tangible measure due to the artifact under study such as workstations (Moore and Benbasat 1991), smart cards (Plouffe et al. 2001), or the nature of the workplace or educational setting (e.g., Agarwal and Prasad 1997; Karahanna et al. 1999), visibility and descriptive norm as described above share some similarities. Both relate to how prevalent the technology appears to be to the individual, yet the operationalization of descriptive norm is more about the belief in how prevalent others' use of the technology is, and not just the perceived visibility of the artifact or technology itself. Lee and Kozar (2005) modified the operationalization of visibility to be more social in nature. Their findings suggest that visibility of the use of anti-spyware by others influences user anti-spyware software adoption intentions. Lee and Kozar's findings related to the social adaptation of the visibility construct combined with the strong body of evidence that visibility of innovations positively influences technology adoption behavior (e.g., Agarwal and Prasad 1997; Karahanna et al. 1999; Moore and Benbasat 1991; Plouffe et al. 2001), and descriptive norm research conducted in psychology (Astrom and Rise 2001; Rivis and Sheeran 2003a) collectively suggest that if an individual believes others are taking precautions to secure their own computers, the individual is more likely to form intentions to take similar precautions with her own computer.

H6b: Descriptive norm is positively related to behavioral intentions to protect one's own computer.

The final proximal determinant of intentions to perform security-related behavior in our model is psychological ownership. The more an individual feels ownership of the hardware, software, and data that is threatened, the higher his/her desire to protect that object. Consumer goods can serve as symbols expressing education, accomplishments, and personal values (Levy 1959). As we interact with possessions, we learn about ourselves and derive comfort and plea-

sure, which increases our self-knowledge and serves to make the possession an extension of the self (McCracken 1986). In the case of an individual's own computer, a sense of psychological ownership is enhanced through controlled use and active association with the computer (Furby 1978). Additional research suggests a relationship between work and effort invested and psychological ownership (Rochberg-Halton 1980). Therefore, we expect investments of time and energy in customizing computer settings and creating files to further increase psychological ownership toward one's computer.

Likewise, while the Internet is not a physical good that consumers take possession of within their homes, it is a network with which individuals interact to accomplish tasks and manipulate their environment. For example, the Internet makes it possible for individuals to communicate via e-mail with family and friends around the world. It enables entertainment, research, and economic activities. Thus, the Internet fulfills the individual's effectance motives, and the related desire to control and possess objects that provide the individual with a sense of causal efficacy (Dittmar 1992; Furby 1978; White 1959). As an individual invests more time and energy performing activities requiring the Internet and actively associating with others via the Internet, she is likely to experience an increased sense of psychological ownership for the Internet.

An increase in psychological ownership for an object will engender heightened protective tendencies toward these targets (Dipboye 1977; Korman 1970). In addition, employees' feelings of psychological ownership toward their job positively influence voluntary, citizenship-type behavior (Dyne and Pierce 2004). Weirich and Sasse (2001) found that an employee's allegiance to the organization was associated with positive password behavior. These results collectively suggest that home computer users' feelings of ownership are likely to be correlated with the voluntary intentions to engage in security-related behavior. The underlying logic is simply that one seeks to protect what one owns and values.

H7a: Psychological ownership of the Internet is positively related to behavioral intentions to protect the Internet.

H7b: Psychological ownership of one's own computer is positively related to behavioral intentions to protect one's own computer.

In sum, we define the conscientious cybercitizen as an individual who is motivated to perform the necessary actions to secure his/her computer and the Internet in a home setting. Building upon and extending PMT, we theorize that in addition to subjective norm and attitude, intentions to perform security-related behavior are influenced by descriptive norm and the sense of ownership and responsibility one feels toward the target artifact. The empirical study conducted to test these research hypotheses is described next.

Methodology and Results: Study 1

Sample and Measures: Study 1

We conducted a field study and collected data for study 1 via a questionnaire. Because the target population for this study is the general public who uses home computers and has access to the Internet, we sampled from multiple subpopulations to ensure a broad representation. These included (1) subscribers of a locally based ISP marketed as a "hometown" provider to a rural community and (2) undergraduate students enrolled in an introductory business course at a large university. In addition, we obtained a sample from a professional survey respondent service.

The survey provides contextual information as appropriate to ensure that each respondent completes it while thinking about his/her home computer and related data, information, or procedures. As noted earlier, evidence suggests that home computer users demonstrate an understanding of common security terms and indicate relatively high usage of commonly recommended security precautions such as the ones we focus on in this study (Furnell et al 2007; Schulman, Ronca, & Bucuvalas, Inc. 2007). However, where necessary, terms are explicitly defined (e.g., security violation, security precaution) to ensure that respondents have a common understanding of each term and understand specifically what violations and which precautions are to be considered for the purposes of the survey (see Appendix A). By providing such descriptions, in the unlikely event that an individual was not previously aware of these specific violations or precautions, they have the informative content necessary for forming attitudes and intentions (Anderson 1981; Jacoby et al. 2002; Zajonc 1968).

Measures were primarily adapted from a variety of previously validated scales, and multi-item scales were used to improve reliability and validity of measurement. Each item involves a statement that is either positive or negative and the respondent utilizes a seven-point Likert scale to indicate his/her level of agreement with the statement. For the constructs largely drawn from PMT—concern about security and perceived citizen effectiveness—we adapted scales from Obermiller (1995), Ellen and Wiener (1991), and Ho (1998) as a starting point and modified them for the security context. We also examined measures used by Culnan (2004) to create these scales. Existing validated scales used by Dyne and

Pierce (2004) were used to measure psychological ownership. For the self-efficacy, subjective norm, attitude, and behavioral intention measures, we adapted scales from Taylor and Todd (1995). Finally, to measure descriptive norm, new items were developed by drawing upon the work of Rivis and Sheeran (2003b).

Since this survey was conducted at the individual level, demographic variables including age, gender, and education level were captured. Other control variables captured included Internet experience, computer experience, exposure to media coverage of security, and prior experience with security violations. Prior experience (both personal and vicarious) with security violations was assessed using adapted scales from measures created and tested by Malhotra et al. (2004) in their privacy research.

Because reliability measures are inconsistently reported across these prior studies and because we developed some additional security-specific items, we conducted a pilot study and obtained 30 responses from graduate students enrolled in a large university in the eastern United States. Based on analysis of the pilot survey data, reliabilities of the various scales exceeded the generally accepted Cronbach's alpha of .7 (Nunnally 1967) with the exception of the scales measuring descriptive norm and perceived citizen effectiveness. Nunnally (1967) argues that a Cronbach's alpha level of .7 is acceptable for confirmatory work while .6 may suffice for exploratory work such as ours. Our scales met these criteria. However, as the scales for descriptive norm consisted of only two items, we adapted the existing items to create two additional items and reworded the items to be more personal (e.g., "I believe...") to potentially improve reliability for the full survey launch. It is likely that the lower reliability of the perceived citizen effectiveness scale was due to a mixture of positively and negatively worded items in the scale and that reliability would likely improve with only positively worded items. See Appendix A for all measurement scales.

Results: Study 1

Prior to testing the full conceptual model, we conducted detailed tests to examine common methods bias and, based on the results, concluded that common methods is not a threat to our findings (see Appendix B.) Across our three groups of respondents, approximately 2,846 individuals received an invitation to participate in the survey and 594 responses were obtained for a response rate of 21 percent.[7] The variety of ways in which we obtained responses yielded a demographic distribution for our sample that is very similar to the demographic distribution of Internet users as detailed in Day et al.'s (2003) report on computer and Internet use in the United States. Table 2 provides our sample demographics alongside demographics for the U.S. Internet population as whole. Over 80 percent of the respondents reported having 6 or more years of computer experience and over 70 percent reported 6 years or more Internet experience. Thus, these respondents are likely to have well-formed perceptions and attitudes about computer security. The overwhelming majority of respondents (91 percent) identified themselves as the primary user of their computer and the person responsible for taking care of the computer (89 percent).[8] To check for non-response bias, early versus late responder data was compared for each subgroup and no significant differences were found between the summated scales for the two groups (Armstrong and Overton 1977). In addition, our sample's demographics compare favorably with those of the Internet user population, which is a common means of estimating non-response error (Sivo et al. 2006). Specifically, the percentage of males in our sample and the age breakdown for individuals 35 and over is almost identical to that of the U.S. Internet user population (Day et al. 2003). Furthermore, as suggested by Rogelberg and Stanton (2007), we control for potential influence of interest level factors such as previous exposure to security violations, which was not significant. Our sensitivity analysis, conducted by removing users not responsible for the computer, also yielded findings consistent with the sample as a whole. Collectively these tests mitigate the potential threat of non-response bias in our results.

Descriptive statistics for the research constructs are shown in Table 3. We conducted extensive analyses to validate the psychometric properties of the measures (see Appendix C). These tests suggest the instrument possesses acceptable psychometric properties. In addition, *post hoc* testing yields statistical power exceeding .95 for our analysis, indicating there is only a .05 chance that we have incorrectly identified a relationship as insignificant when, in fact, it was significant (i.e., type II error).

[7]The breakdown of our sample by subgroup is 157 (26.4 percent) from the ISP, 94 (15.8 percent) from the undergraduate pool and 343 (57.7 percent) from the purchased sample. We obtained response rates for the ISP, undergraduate, and purchased sample of 11.2 percent, 26.9 percent, and 31.3 percent respectively.

[8]With the 11 percent of users who indicated they were not responsible for their computers removed from the sample, our results hold with the exception of attitude, which becomes insignificant at predicting Intentions to protect the Internet. We retain these users in our sample because the behaviors of interest in our study are not restricted just to activities such as computer maintenance tasks (e.g., purchasing and installing antivirus software) that might be exclusively performed by the responsible user but also include exercising care when opening e-mail attachments and the use of strong passwords that are important behaviors for all computer users.

Table 2. Demographics for Sample and U.S. Internet Population

Demographic Characteristic	Sample	U.S. Internet Population*
Age		
18–24	25%	15%
25–34	12%	21%
35–44	22%	24%
45–54	22%	21%
55–64	12%	12%
65 and over	7%	7%
Education		
Some school, no degree	2%	5%
High school	13%	25%
Some college, no degree	37%	33%
Associate's degree	9%	
Bachelor's degree	25%	25%
Master's degree	10%	12%
Doctorate	4%	
Gender		
Male	47%	48%
Female	53%	52%

*Census Computer and Internet Use in the United States: 2003 (http://www.census.gov/population/www/socdemo/computer/2003.html)

Table 3. Descriptive Statistics

Construct	Mean	S.D.
Concern	5.17	1.19
Perceived Citizen Effectiveness	4.86	1.17
Self-Efficacy	5.10	1.27
Security behavioral attitude	6.35	0.84
Subjective Norm	4.73	1.45
Descriptive Norm	4.74	1.21
Psychological Ownership for Own Computer	6.20	1.25
Psychological Ownership for Internet	3.44	1.63
Security Behavioral Intention (Own Computer)	6.16	0.98
Security Behavioral Intention (Internet)	5.50	1.32

Notes: All constructs are seven-point scales. Self-Efficacy anchors: 1 = Not at all sure, 7 = Very Confident. Perceived Coping Response Efficacy anchors: 1 = Not at all Effective, 7 = Very Effective. Probability of Occurrence anchors: 1 = Highly Unlikely, 7 = Highly Likely. Prior Experience anchors: 1 = Very Infrequently, 7 = Very Frequently. All other constructs anchored with 1 = Strongly Disagree, 4 = Neutral, 7 = Strongly Agree.

We used partial least squares (PLS) estimation for the full model. All constructs were modeled as reflective with the exception of the concern construct, which was modeled as formative. To eliminate potential confounding of results due to specific individual characteristics, a respondent's gender, age, education, Internet experience, computer experience, prior experience with security violations, and media exposure to security violations were included in the analysis as controls. The results of the PLS analysis are reported in Figure 2. Media exposure, Internet experience, computer experience, and prior experience with security violations were not significantly related to either attitude or intentions and were dropped from the model. Age and gender were significantly related to attitude, and age and education were significantly related to behavioral intentions to protect the Internet. These variables were included in the model to partial out such differences.

As summarized in Table 4, all hypothesized paths are supported with the exception of H5a and H6b. The model explains 43 percent of variance in intentions to secure one's own computer and 35 percent in intentions to secure the Internet. Subjective norm, or what an individual believes others think he/she should do, influences an individual's protective behavior toward his/her own computer but not the Internet as a whole, whereas the reverse is true for descriptive norm. That is, consistent with the notion that the Internet can be conceived of as a public good, and that individuals are more likely to take action when they believe others are doing the same, descriptive norm influences protective behavior toward the Internet but not their own computer.

As predicted by PMT, an individual's attitude toward security-related behavior is influenced by concern regarding security threats, perceived citizen effectiveness, and self-efficacy. Consequently, to be simply concerned about security is insufficient: individuals must also believe in their ability to take the necessary precautions, and that the precautions will actually make a difference. The more positive an individual's attitude, the higher his/her intentions are to take action to protect both his/her own computer and the Internet as a whole.

Finally, individual intentions to protect the Internet and one's own computer are influenced by attitude, social norms, and psychological ownership. Although the specific social norms influencing intentions are different across the two targets, the findings support the existence of a social component in the formation of such intentions. Psychological ownership also plays a role in the formation of intentions. The greater the sense of ownership an individual feels for his/her computer, the higher are his/her intentions to protect it. Likewise, the greater the sense of ownership an individual feels for the Internet, the higher are his/her intentions to take action to protect the Internet.

Limitations: Study 1

Prior to discussing the findings of study 1, we acknowledge its limitations. The survey is based on self-reported information, which may be subject to common methods bias. However, the single-factor and other common method factor tests indicate that this bias does not pose a threat to our findings (Podsakoff et al. 2003; Williams et al. 2003). We administered the survey to a subset of individuals in the United States. Nonetheless, the sample demographics closely match the population of Internet users in the United States (Day et al. 2003), indicating that the sample serves as an adequate representation of home computer users. We assessed intentions rather than actual behavior. However, actual behaviors are difficult to study in the security context (Vroom and von Solms 2004). Furthermore, the relationship between intentions and actual behavior is not only an association grounded in several widely used theories such as TBP and TRA (Ajzen 1991; Fishbein and Ajzen 1975), but it has also been shown to be strong and consistent (Venkatesh et al. 2003) based on correlational tests of intention–behavior consistency (Sheeran 2002), as well as meta-analytic tests conducted based on experimental studies examining the impact of changing subject intentions on subsequent behavior (Webb and Sheeran 2006). Nonetheless, future studies should endeavor to assess users' actions with respect to security. Finally, while a large portion of the sample possesses a high level of experience with computers and the Internet, we did not explicitly test respondents' knowledge of how to implement the security precautions relevant to our study. This variable could potentially moderate the intention–behavior relationship. In addition, the experience levels of this particular sample may make them more sensitive to security. Studies with additional samples, including samples outside the U.S., are necessary to further generalize the findings.

Discussion: Study 1

Study 1 was designed to address our first two research questions involving an improved understanding of home computer user's security behavior. Five of the seven hypotheses were supported by the data. The other two were supported for one of the two dependent variables, that is, intentions to protect the Internet or one's own computer, but not for both. Theoretically, findings validate the appropriateness of an extended version of PMT, which incorporates consideration of the fact that the target of protection, one's computer and

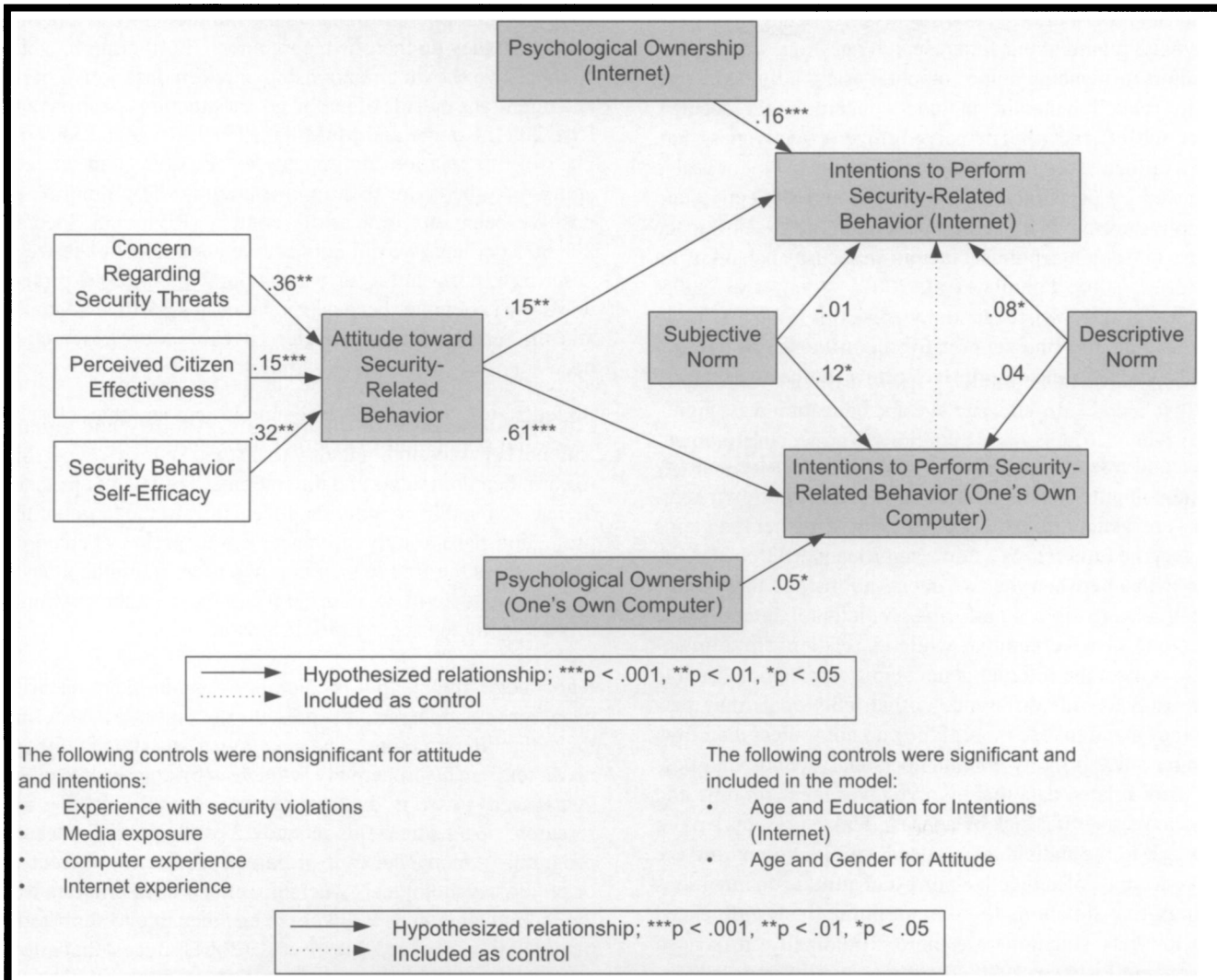

Figure 2. PLS Results: Study 1

Table 4. Results by Hypothesis

Hypothesis	Support?
H1: Concern ➔ Attitude Toward Security-Related Behavior	Yes
H2: Perceived Citizen Effectiveness ➔ Attitude Toward Security-Related Behavior	Yes
H3: Self Efficacy ➔ Attitude Toward Security-Related Behavior	Yes
H4a: Attitude ➔ Intentions to Perform Security-Related Behavior (Internet)	Yes
H4b: Attitude ➔ Intentions to Perform Security-Related Behavior (Computer)	Yes
H5a: Subjective Norm ➔ Intentions to Perform Security-Related Behavior (Internet)	No
H5b: Subjective Norm ➔ Intentions to Perform Security-Related Behavior (Computer)	Yes
H6a: Descriptive Norm ➔ Intentions to Perform Security-Related Behavior (Internet)	Yes
H6b: Descriptive Norm ➔ Intentions to Perform Security-Related Behavior (Computer)	No
H7a: Psychological Ownership (Internet) ➔ Intentions to Perform Security-Related Behavior (Internet)	Yes
H7b: Psychological Ownership (Computer) ➔ Intentions to Perform Security-Related Behavior (Computer)	Yes

the Internet, is not the self, to study security behavior. Specifically with regard to our first research question, we find that the factors influencing home computer users' attitude toward security-related behavior include concern about security threats, self-efficacy, and perceived citizen effectiveness that, in turn, influence security behavior. Security behavior is also influenced by psychological ownership and subjective and descriptive norms. While others have examined the influence of threat and coping appraisal factors on security behavior (La Rose et al. 2008; Pahnila et al. 2007; Woon et al. 2005; Workman et al. 2008), to our knowledge, this is the first study to investigate and find support for the influence of psychological ownership and descriptive norm on home user security behavior.

Our second research question asked if the factors influencing a home computer user's intentions to protect her own computer were distinct from the factors influencing her intentions to protect the Internet. We find a significant difference in the relationships between the two social norms and intentions. Subjective norm is a significant predictor of intentions to protect one's own computer, while its relationship to intentions to protect the Internet is not significant. One plausible explanation for this difference is that individuals may perceive they stand to lose more if they do not protect their own computer since it likely contains personal, school, and possibly work-related data that involve investments in time and money to recover if struck by a virus. This represents a more direct risk to the individual. Indeed, studies comparing the relative weights of subjective norm and attitude on intentions find high-risk situations to be more normatively influenced while low-risk situations are more attitudinally influenced (Stasson and Fishbein 1990; Trafimow and Fishbein 1994). Furthermore, individuals may believe more strongly that it is their role to protect their computer, while the responsibility for protecting the Internet is one that is jointly held with all other Internet users. The stronger an individual's identification with a particular role, the higher the probability that his behavior will be consistent with that identity. A study of blood donors found that once role identity salience and social relations were accounted for, the influence of subjective norm on intentions varied over time in predicting repeated behaviors (Charng et al. 1988). It may be that the inclusion of descriptive norm in our model also shifts the importance of the norms-intention relationships.

Conversely, the relationship between descriptive norm and intentions to protect the Internet is significant, but not the relationship to intentions to protect one's own computer. One possible explanation for the salience of descriptive norm only for the Internet is that what others are doing has been shown to be important in public good scenarios (Frey and Meier 2004; Keser and van Winden 2000; van Dijk and Wilke 1997), and individuals perceive the Internet more as a public good than they do their own computers. Furthermore, while studies have shown a relationship between descriptive norm and intentions outside of public goods situations (Astrom and Rise 2001; Conner and McMillan, 1999; Rivis and Sheeran 2003b), this relationship appears to be stronger in encouraging risky behavior than in encouraging the promotion of positive behaviors in a health context (Rivis and Sheeran 2003a). Perhaps, we did not observe a relationship between descriptive norm and security behavioral intentions to protect one's own computer because the latter is a positive behavior and the relationship is, therefore, weak. More research is necessary to explore this possibility.

Finally, consistent with findings in psychology and organizational behavior, individuals vary in their sense of ownership toward their computers and the Internet. The level of psychological ownership an individual feels toward the target of the protection also strongly influences his/her security behavior. Our study is the first to examine two targets simultaneously in order to determine if differences exist in the proximal drivers of home user security behavior.

Knowledge about the predictors of individual security behavior in a home setting represents the first step in securing the cyber infrastructure. The next logical question is if these predictors can be proactively *influenced* by appropriate interventions, as posed in the third research question driving our research. We address this in study 2 of the phased research program. Among the four proximal predictors of security behavior, psychological ownership reflects an internal state of the individual that is less likely to be amenable to short-term manipulations. Indeed, Pierce et al. (2001) suggest that information alone is likely insufficient to build psychological ownership. In order to create or sustain psychological ownership, a level of intensity of interaction with the target of possession is required over a period of time. In contrast, norms and attitudes are more malleable and can be altered through messages conveyed via public awareness campaigns, or in software vendor advertisements. In addition to informative messages about risks and appropriate responses, public service campaigns could be designed to utilize varied referent groups in order to invoke the salience of different social norms.

In summary, a variety of cognitive and psycho-social components influence the security behavior of home computer users. Our findings suggest that it is not just awareness about threats and coping responses that influence behavior, but that there are also social norms and psychological factors to consider when attempting to motivate home computer users. To investigate what type of message cues are likely to influence norms and attitudes in the context of home security behavior, we conducted a follow-on study, described below.

Additional Theoretical Background and Hypotheses: Study 2

In study 2, we build on our understanding of user motivations and attempt to influence user security attitude and norms. Specifically, our goal is to determine the most effective mix of *message* qualities that would have a positive effect on home computer attitude toward security-related behavior, and amplify subjective and descriptive norm. The marketing and economics literature is rich with research that explores the factors influencing decision making and choice behavior. In this literature, the manner in which the information presented to an individual is framed has recurrently been identified as a key driver of attitudes and behaviors. In addition, since the findings of study 1 suggest a social component to security behavior, a manipulation that primes individuals to focus on different referent groups to influence the social norms invoked might prove effective. One such mechanism is the manipulation of self-view to prime individuals toward an interdependent versus independent view.

Drawing upon research in marketing, psychology, and economics, we apply concepts of goal framing and self-view to investigate how attitudes and norms can be manipulated. In the context of this study, framing of a message serves to focus the individual either on preventing the threat and associated negative outcomes of a security violation (negative, or prevention, frame), or on the utilization of effective coping responses in order to create a safe, reliable Internet environment (positive, or promotion, frame). The self-view manipulation serves to shift an individual's frame of reference toward either an interdependent self or independent self. A shift in the frame of reference alters the individual's referent group which, in turn, influences the social norms that become salient for the individual.

Through an experiment conducted on 101 subjects using a 2 (promotion versus prevention goal frame) × 2 (independent versus interdependent self-view) factorial design, we demonstrate that home computer user attitudes and norms can be influenced by message manipulations. Our findings have practical implications which can benefit organizational social marketing efforts. They may also be useful for vendors desirous of creating effective advertising for security-related software and hardware. This study makes theoretical contributions to the literature by providing insight into the mechanisms underlying self-view and goal frame influences on outcomes as consumer attitudes, intentions, and choices (Aaker and Lee 2001; Hamilton and Biehal 2005; Lee et al. 2000).

We begin with a brief review of the relevant literature, including the study hypotheses. The methods are described next, followed by the results. After a discussion of the implications of the findings from study 2, we interpret the combined results of studies 1 and 2.

Framing and Goals: Study 2

A number of studies have drawn upon prospect theory (Tversky and Kahneman 1986) to assess the influence of positively versus negatively worded messages on decision-making behaviors (e.g., Aaker and Lee 2001; Block and Keller 1995; Hamilton and Biehal 2005; Maheswaran and Meyers-Levy 1990; Shiv et al. 2004). Tversky and Kahneman (1986) proposed prospect theory as a means of explaining circumstances where individual behavior does not conform to theories of rational choice. Prospect theory describes the process of choice as consisting of a framing and editing phase, followed by an evaluation phase. The manner in which a message is framed influences choice behavior even when the message conveys essentially the same information (Aaker and Lee 2001; Lee and Aaker, 2004; Tversky and Kahneman 1984). During the evaluation phase, individuals evaluate alternatives partially based on their respective values in terms of whether an option is perceived to be a loss or a gain. The value function used in prospect theory indicates a response to losses that is more extreme than the response to gains, and is referred to as *loss aversion* (Tversky and Kahneman 1984). Messages that emphasize the negative outcomes of a choice are perceived as potential losses, which individuals are likely to want to avoid more than their desire to realize a potential gain, described in a message that emphasizes the positive outcomes (Tversky and Kahneman 1984).

Over time, research investigating loss aversion in the context of decision making and choices under risk has yielded variations in findings (e.g., Takemura 1994; Wang 1996). These variations have been attributed to what Levin et al. (1998) call *framing* effects. In an effort to better understand the inconsistent results achieved in the various studies, Levin et al. conducted a review of framing effect studies and proposed a typology of framing effects. They categorized previous studies into three different types of framing manipulations: risky choice framing, attribute framing, and goal framing. In a risky choice framing, options are presented as differing in their level of risk. Attribute framing involves describing an object or event differently. Finally, goal framing assumes both frames are good in that there are benefits implied in both the positive and negative frames, and involves emphasizing either the positive aspects of a behavior, or the negative aspects of not performing the behavior. Because goal framing is often applied in persuasive communications and since our objective is to determine what type of communication is effective in increasing home com-

puter users' intentions to behave in a secure fashion online, we restrict our focus to goal framing.

Goal framing effects have been studied from economics, marketing, and social psychology perspectives in a variety of decision contexts such as those related to health (Dutta-Bergman 2004), social dilemmas (Brewer and Kramer 1986), and finances (Tversky and Kahneman 1981). Scholars have examined the influence of message framing on numerous dependent variables including attitudes and intentions (Block and Keller 1995; Maheswaran and Meyers-Levy 1990), perceived importance and favorability of message (Aaker and Lee 2001; Lee et al. 2000), risk perceptions (Lee and Aaker 2004), and choices and goals (Hamilton and Biehal 2005). In the current study, the dependent variables of interest are subjective norm, descriptive norm, and attitude toward security-related behavior. Although research has examined the influence of goal frame on attitude, the results have been inconsistent, which has led researchers to examine moderating variables (Block and Keller 1995; Lee and Aaker 2004; Maheswaran and Meyers-Levy 1990). Consequently, we do not hypothesize direct effects of goal frame on attitude but, rather, examine its effect on attitude in conjunction with self-view as a moderator. There is no prior research or compelling theory suggesting a direct effect of goal frame on norms.

The Role of the Self in the Context of Others on Individual Choice: Study 2

Goal framing and prospect theory both have a predominantly individual focus, and are largely cognitive in nature (Tversky and Kahneman 1984). An assumption implicit in these theories is that individuals process all available information using the *self* as the locus of evaluation (Tversky and Kahneman 1984). Thus, they do not directly address the social aspects that pervade certain types of decisions (van Dijk and Wilke 1997). Arguably, use of the Internet is inherently social in nature as individuals correspond via e-mail, make purchases partially based on expert and consumer reviews, and share information via bulletin boards, list services, blogs, and the like. The decision to practice secure online behavior has ramifications not only for an individual but also for all others accessing the shared resources of the Internet (Noyes 2007; Symantec 2009). As established in study 1, social factors are an important component in the formation of security-related behavior. Specifically, subjective norm, which is what an individual believes others expect him to do, and descriptive norm, which is what an individual believes others are doing, influence home computer user security behavior.

Prior literature provides evidence for the influence of the awareness of others and their actions on choice behavior. For example, in antismoking campaigns aimed at adolescents (Pechmann et al. 2003), peer pressure and the desire to be accepted influences smoking decisions. Individuals choose to contribute in social dilemmas for the benefit of the common good when free-riding may hold more benefit to the individual personally (Andreoni 1995; van Dijk and Wilke 1997). Finally, an individual's self-view, whether she thinks of herself as independent or interdependent, influences choice behavior (Aaker and Lee 2001; Hamilton and Biehal 2005). An individual with a dominant independent self-view thinks of herself as unique and separate from others while an individual with a dominant interdependent self-view values his position within a group (Singeles 1994). It is generally believed that the former self-view is fostered in Western cultures such as the United States while the latter is nurtured in Eastern cultures such as China (Singeles 1994). However, research has shown that a particular self-view can be made temporarily accessible through message primes (Aaker and Lee 2001; Hamilton and Biehal 2005).

The effects on choice behavior are, arguably, influenced by the norms made salient by such messages. We chose to attempt to shift the salient referent group via self-view manipulations, which involve priming an individual to either think of herself as distinct and separate from others (independent), or to think of herself as part of a larger group (interdependent). By manipulating the self-view, an individual's referent group is modified. The larger and more closely connected the referent group is perceived to be, the more salient certain norms may be. Therefore, we expect self-view manipulations to influence the level of subjective and descriptive norms reported by subjects, depending on whether they are primed with an interdependent or independent self-view. Moreover, studies have shown an interactive effect of self-view and goal frame on attitudes, intentions, and choice behavior (Aaker and Lee 2001; Lee et al. 2000). Below, we briefly summarize the relevant literature on this interaction to derive specific research hypotheses.

Self-View and Goal Frame Interaction: Study 2

As described previously, self-view and goal frame manipulations are likely to influence social norms and attitudes toward performing a particular behavior. In order to hypothesize the influence of these two manipulations in combination, we draw upon prior research which has investigated the interaction of self-view and goal frame. Studies have found that subjects primed with an independent self-view are more attuned to promotion-focused messages while subjects primed with an interdependent self-view attend and respond more to prevention-focused messages (Aaker and Lee 2001; Lee et al. 2000). The state in which one's active self-view (indepen-

dent/interdependent) and the goal (promotion/prevention) frame are consistent is called a goal *compatible* condition, which leads to increased persuasive effects (Aaker and Lee 2001). Goal compatible conditions yield more favorable attitudes toward brands, increased perceived effectiveness of web sites, and improved recall of information (Aaker and Lee 2001). Therefore, we expect a goal compatible message condition to result in a more favorable attitude toward performing security-related behavior.

H8: Self-view and goal frame manipulations interact to influence attitude toward performing security-related behavior. Specifically, subjects primed with an independent (interdependent) self-view will report a more favorable attitude toward performing security-related behavior when receiving a promotion-focused (prevention-focused) goal frame than subjects primed with a prevention-focused (promotion-focused) goal frame.

Although we are not aware of any prior examination of norms in a goal compatible context, self-view manipulations serve to focus an individual's attention on themselves or others, which is likely to shift one's referent group and associated salient norms. To the extent that goal compatible conditions lead to improved recall of information that is relevant (Aaker and Lee 2001), and a perception that the message is more important (Lee et al. 2000), it follows that relevant norms would be similarly enhanced. Therefore, we test

H9: Self-view and goal frame manipulations interact to influence subjective norm. Specifically, subjects primed with an independent (interdependent) self-view will report a higher level of subjective norm when receiving a promotion-focused (prevention-focused) goal frame than subjects primed with a prevention-focused (promotion-focused) goal frame.

H10: Self-view and goal frame manipulations interact to influence descriptive norm. Specifically, subjects primed with an independent (interdependent) self-view will report a higher level of descriptive norm when receiving a promotion-focused (prevention-focused) goal frame than subjects primed with a prevention-focused (promotion-focused) goal frame.

Methodology and Results: Study 2

To test these research hypotheses, we conducted an experiment in a laboratory setting employing a 2 × 2 (message framing: promotion or prevention × self-view: independent or interdependent) between-subjects factorial design. As explained below, the framing of the message and the self-view embedded in it were manipulated via asking the subjects to review a website that differentially emphasized positive and negative consequences, and individual or collective themes.

Message Framing Manipulation

Subjects were randomly asked to review a website containing a security message that is positively (promotion-focused goal) or negatively (prevention-focused goal) worded. The positively worded message focuses on the *benefits* of performing security precautions such as reliability, stability, and peace-of-mind for both individuals and organizations. The negatively worded message stresses the consequences of not taking security precautions, thus focusing on the severity and probability of threats.

The four website conditions are shown in Appendix D. The content of the websites is based on examples of descriptions of risks and benefits to practicing secure behavior across non-profit websites such as the Department of Homeland Security, National Cyber Security Alliance, and EDUCAUSE. In addition, we reviewed relevant websites hosted by security-related software vendors such as Symantec/Norton, Microsoft, and McAfee. The website manipulations represent an effort to consolidate common themes to create strong positive and negative content. To control any possible decision-making heuristic biases due to the volume of message content, the messages are of comparable length in terms of number of words and paragraphs.

Self View Manipulation

The messages on the websites are worded so as to focus either on the individual (e.g., *yourself*, *your* data, *your* personal productivity, etc.) or on the individual as part of the Internet community (e.g., *all* interconnected users of the Internet, the *community*, etc.). Graphics are also used to reinforce the individual versus interdependent view.

Main Study Procedure and Variable Operationalization

Recall that in study 1 our target population was any user of an Internet-enabled computer who is not directly subject to job-related consequences as a result of acting in an unsecure

fashion online, and our sample was drawn accordingly. In study 2, our sample consists of undergraduate students from a large university enrolled in a required marketing course. As a result, it represents a narrow demographic segment of that population, the 18 to 24 year olds. We believe it is especially important to understand how to influence this segment of users as they represent a significant proportion of current and future Internet users (Day et al. 2003).

A total of 101 subjects participated in the experiment. Random assignment of subjects to conditions resulted in 25 subjects for conditions 1 (independent/prevention), 3 (independent/promotion), and 4 (interdependent/promotion), and 26 subjects in condition 2 (interdependent/prevention). The random assignment of subjects to conditions improves the distribution of individuals with varied backgrounds to reduce any systematic influence due to factors we do not explicitly control. Participants were isolated from each other and completed the experiment independently as part of a set of unrelated experiments for which they received extra credit in an undergraduate marketing course. Participants signed up in advance for a session on a volunteer basis, and alternative assignments were available for students preferring not to participate in experimental research. Subjects participated in computer labs equipped with computers that enable them to access the experimental scenarios and respond to the post-questionnaire electronically. The laboratory setting ensures an environment that is consistent across all participants and free of distraction. No interaction is allowed between participants during the session.

Participants were instructed to take their time reviewing the website and then proceed to the questionnaire portion of the study. After each participant read the website, an online questionnaire including manipulation check questions and multi-item scales measuring the dependent variables including subjective norm, descriptive norm, and attitude toward performing security-related behavior was completed. We used the same scales as in study 1, with the exception of attitudes that are measured separately for one's own computer and the Internet. Where necessary, terms such as security violation and security measures were explicitly defined so that each respondent had a common understanding of each term (see Appendices A and D).

As before, since this study involved individual-level perceptions, we collected demographic information such as gender, age, education, and years of computer and Internet experience. In addition, the subjects were asked to indicate how much they heard or read about computer security recently in order to assess any influence of prior media exposure as well as past security violations.

Results: Study 2

Males accounted for 52 percent of the study subjects. There were no significant differences in any of the demographic or control variables across the four conditions, indicating that random assignment had achieved the desired equivalence between groups.

Manipulation Check

As a manipulation check, subjects completed several questions regarding their thoughts immediately after reviewing the website(s). The questions focused on determining the extent to which the subject was thinking about the benefits or consequences of security violations and the extent to which the subject was thinking about self as compared to thoughts about others (see Appendix E). A repeated measures ANOVA shows the anticipated effect of goal frame on thoughts about negative consequences versus benefits ($F_{1,97}$ = 11.225, p = .001). The partial eta-squared estimate of effect size for this relationship is .105.

The repeated measures ANOVA on the self-view condition failed to show the anticipated effect of self-view on thoughts about self versus others ($F_{1,97}$ =0, p = .983). Although the self-view manipulation check failed, it can be seen (based on the ANOVA results described below to test the hypotheses) that self-view does significantly influence some of the study's proposed mediating and dependent variables. Since self-view influences the dependent variables, it may be that the self-view manipulation is more subtle than could be assessed by the manipulation check questions. According to Sigall and Mills (1998), the questions we use constitute an independent variable check and not a treatment check. A treatment check would have asked the respondents if they noticed that the website referred to an individual and his/her actions versus groups of people and their collective actions (similar to the wording of the goal frame manipulation checks), and may have served to sensitize respondents to our experimental treatments. An independent variable check is intended to assess the conceptual independent variable (in our case, self-view), and is harder to obtain as it is more subtle. Sigall and Mills note it would be inappropriate to exclude participants based on responses to an independent variable check, and that differences on mediating and/or dependent variables can be taken as evidence that the treatment was noticed.

To confirm the self-view priming manipulation successfully influences thoughts about the self and the self in the context of others, we conducted a *supplemental* test with two conditions identical to the independent and interdependent condi-

tions used in the main experiment. We recruited an additional 28 undergraduate subjects for this test using an identical recruiting procedure as with the main study, and conducted an experiment replicating the procedures of the main study. For this supplemental test, we altered the manipulation check questions to specifically ask the subject to describe the extent to which the website (1) made the subject think about the impact of security issues on just the self, (2) focused the subject's thoughts about the message on just the self, (3) made the subject think about the impact of security issues on self and other interconnected users of the Internet, and (4) focused the subject's thoughts about the message on self and the Internet community of users. The wording of these questions is consistent with the manipulation checks used to assess the success of the self-view prime by Aaker and Lee (2001). A repeated measures ANOVA shows the anticipated effect of self view on thoughts about the self versus thoughts about the self and other users of the Internet ($F_{1,26} = 11.025$; $p = .003$). Participants given the independent condition thought more about just the self ($M = 5.063$) than the self with other Internet users ($M = 3.813$), while participants receiving the interdependent condition thought more about themselves with other Internet users ($M = 4.708$) than they thought about just themselves ($M = 3.792$). The partial eta-squared estimate of effect size is for this relationship is .289.

Psychometric Properties of Scales

We first assessed the convergent and discriminant validity of the multi-item scales using principal components factor analysis with varimax rotation and next examined the reliability of the scales (see Appendix F). These tests suggested the instrument possesses acceptable psychometric properties. We created indices for all of the dependent and independent measures for further analysis.

ANOVA Results

A two-way ANOVA (self view × goal frame) indicates no significant influence of the interaction of self view and goal frame on either attitudes relating to protecting one's own computer or the Internet (see Table 5). Thus, hypothesis 8 is not supported. Due to the insignificant results, we examined observed power and found it to be particularly low for the tests related to the attitude variables (see Table 5). Calculations of *post hoc* effect size using Cohen's *f* (Cohen 1988) show that the effect sizes obtained (.08 and .16) are quite small since, according to Cohen, a small effect size for the *f* statistic is .10. As is customary for *ex ante* determination of power when a body of prior research exists on which to base an estimated effect size index (Baroudi and Orlikowski 1989; Mazen et al. 1987), we determined *a priori* cell size for our experiment based on effect sizes obtained in similar experiments conducted in marketing settings upon which the study is based (Aaker and Lee 2001; Hamilton and Biehal 2005; Lee et al 2000). Unfortunately, our results did not replicate the findings previously obtained in other settings. While these results are somewhat surprising as self view and goal frame message cues have been examined and found to significantly influence brand attitudes with similarly sized cells (Aaker and Lee 2001; Lee et al 2000), one explanation is that our study represents an innovative application of these concepts to a unique context (security/information systems). The low power associated with the attitude tests combined with our insignificant results makes it difficult to draw any conclusions related to hypothesis 8. With the effect sizes obtained and a significance criteria of .05, the cell sizes required to attain power of .80 and, thus, appropriate confidence in any insignificant results, would exceed 100 for the attitude (own computer) variable and 400 for the attitude (Internet) variable.[9] The high degree of investment in time and effort required to achieve this level of subject involvement is questionable.

Analyses of the interactive influence of self view and goal frame on subjective norm suggest that message cues make a difference in the levels of subjective norm reported by subjects. A two-way ANOVA (self view × goal frame) with subjective norm as the dependent variable approaches significance ($p = 0.066$) and the observed power of .75 is close to the accepted standard of .80 (Cohen 1988) (see Table 5). Follow-up contrasts show that subjects primed with the independent self-view experience significantly different levels of subjective norm based on the goal frame. Specifically, subjects primed with the independent self view and promotion-focused goal report a significantly higher subjective norm ($M = 5.64$) when compared to subjects primed with the independent self view and prevention-focused goal ($M = 4.75$, $p = .017$). Subjects primed with the interdependent self-view indicate no significant differences in subjective norm based on goal frame. The *post hoc* effect size ($f = .31$) is in the medium range according to Cohen's definition for the *f* statistic (medium effect size is .25). Although our findings related to hypothesis 9 do not achieve significance, they nevertheless suggest an interactive relationship between goal frame and self view on subjective norm, which might have been significant had we obtained a larger sample size.

A similar analysis shows that the interaction of self view and goal frame significantly influences descriptive norm (see Table 5), which supports hypothesis 10. As predicted, descriptive norm is highest for subjects primed with an inde-

[9]Obtained using Table 8.4.4 from Cohen (1988) and nonlinear interpolation.

Table 5. Summary ANOVA Results

Hypothesis/Dependent Variable	Mean Square	F-Statistic†	P-value	*Post Hoc* Effect Size*	Observed Power**	Support?
H8: Self-View × Goal Frame → Security Behavioral Attitude (Own Computer)/(Internet)	.522/1.650	.25/1.17	.617/.283	.08/.16	.09/.24	No
H9: Self-View × Goal Frame → Subjective Norm††	5.631	3.50	.066	.31	.75	No
H10: Self-View × Goal Frame → Descriptive Norm	6.585	4.30	.041	NA	NA	Yes

NA = Not Applicable

*Using Cohen's ***f*** statistic for analysis of variance. **Output obtained from SPSS.

†For each ANOVA reported in Table 5, the F-ratio was calculated with 1 degree of freedom for the effect and 97 for the degrees of freedom for the residuals of the model.

††Follow up contrasts show that subjects primed with the independent self-view report significantly different levels of subjective norm depending on goal frame (p = .017)

pendent self view when presented with the promotion-focused goal frame. A table of means and graphs of the interactions are provided in Appendix G.

Limitations: Study 2

This study was conducted on undergraduate students and, as a result, care should be taken in generalizing these findings to other groups. It is possible that different demographic groups may find different types of messages persuasive. Arguably, however, it is important to understand how to reach college students as they represent a significant portion of the Internet user population that is highly connected and has a tendency to engage in risky behaviors. These users also represent the future of the Internet community (Day et al. 2003).

Discussion: Study 2

The goal of study 2, the second phase of our sequential research process, was to address the third research question and determine the efficacy of different message types in amplifying the proximal drivers of home computer users' security behavior. Building upon research from economics, marketing, and social psychology, we argued that it is possible to influence the security behavior of home computer users with messages that differentially emphasize self view and goal frame. These effects are manifest via the mediating influence of attitudes and the social norms made salient to the user. Although only one of our three hypotheses was supported (H10), the results relating to a second (H9) are in the hypothesized direction, and the *post hoc* power analysis suggests that with a slightly larger sample size the results would likely have reached significance. Theoretically, our study adds to the literature by isolating the impacts of the interaction between goal framing and self view on subjective and descriptive norms. While the amount of rigorous academic research in the security domain is increasing, as evidenced by the studies listed in Table 1, only one has examined the type of messages that can be utilized to influence behavior (La Rose et al. 2008), and that study examined manipulation of personal responsibility. As suggested by the findings of study 1, the factors influencing home user security behavior are numerous, warranting study of a variety of potential mechanisms for improving this important behavior.

Although most messages targeted at improving individual online security behaviors tend to emphasize the potential *negative* consequences of not acting in a secure fashion, which would be consistent with a loss aversion or prevention approach (e.g., Chestnut 2004; Federal Trade Commission 2002), a striking finding of our study is that messages focused on the positive consequences (promotion-focused goal frame) of performing the behavior may actually be more persuasive in the context of online security behavior. This is especially true if that message is conveyed in combination with an individual self view. Furthermore, our results suggest that security attitude may be particularly resistant to message manipulation, but the norms made salient in the context of

online security behavior can be manipulated with the appropriate marketing messages to influence security behavior. Finally, this study demonstrates that the content and framing of the message is highly influential. It is also likely the target demographic is important, warranting further research in this area. Overall, this experiment contributes to a nascent stream of information systems literature that examines user security behavior and its antecedents. It takes the understanding of what motivates a user to behave in a secure fashion and uses it to frame a message aimed at amplifying the incidence of the desired behavior.

Conclusion and Implications

Concerns related to security continue to escalate in importance as the diffusion of Internet accelerates (Symantec 2009). To the degree that the Internet is a critical component of infrastructure that sustains individuals, companies, and nations, its security is of paramount social and economic significance. Even short outages in the network can lead to significant productivity and financial losses (Borrus 2005; Campbell et al. 2003; Garg 2003; Krebs 2005). As we argued here, technology and related procedures are not sufficient in achieving the required sense of security: people must be motivated to utilize the available security technology and consistently perform the necessary procedures.

Individual home computer users represent a significant point of weakness in achieving security of the Internet because they are not subject to training as are employees within organizations, nor are they protected by a technical staff dedicated to keeping software and hardware current. As a result, determining what factors influence individual security behavior is essential. Our results indicate that a home computer user's intentions are formed by a combination of cognitive, social, and psychological components. Furthermore, these intentions can be enhanced through self-view and goal-frame message manipulations focused on the social norms made salient to the user. Interestingly, our findings suggest the most effective messages in the context of online security behavior may be ones that focus on the positive outcomes (promotion-focused goal frame) of performing the behavior and not the more commonly used messages, which focus on the potential negative consequences of not acting in a secure fashion. With an understanding of what impacts security behavior, organizations will be better able to create effective messages to increase the desired security behavior, thus enabling us to continue to rely on the availability of information provided by the Internet, the capability to conduct e-commerce transactions, and to communicate with people around the world.

Implications for Research

Our two studies contribute in a number of ways, summarized in Table 6, which we discuss in turn. First, the two studies offer four theoretical implications for research by extending the existing literature on both protection motivation and persuasive messaging. We note that our core theoretical contribution involves extending PMT to include an explicit consideration of the target of protection through the addition of psychological ownership of the target, and the influence of descriptive norm from the public goods literature. PMT was originally developed and tested in the context of protecting oneself from personal harm (e.g., Ho 1998, Pechmann et al. 2003, Rippetoe and Rogers 1983). While its tenets hold in the security context, we have shown that the application of PMT to the security context is enhanced when consideration is given to factors that acknowledge that security threats target inanimate objects and not the self. It is intuitively appealing that one will seek to protect what one owns, and that protective behaviors will be amplified the greater the sense of ownership. The psychological ownership construct offers considerable explanatory power in both home, as demonstrated by our findings, and organizational settings, as shown in prior research (Dyne and Pierce 2004). The perceived behavior of others is also an important consideration in individuals' behavior (Lee and Kozar 2005; Rivis and Sheeran 2003a). When the target object of security behavior was the Internet, descriptive norm influenced individuals' security behavior while subjective norm influenced security behavior when the target was one's own computer. Thus, our findings further suggest that the proximal drivers of security behavior vary depending on the target of protection. An implication for future research is the need for specificity in the focal target being studied (e.g., a laptop, data stored digitally, a network) because individuals vary in the extent to which they feel a sense of ownership toward different objects and because the factors influencing behavior vary depending on the target.

While we find evidence that the level of psychological ownership an individual feels for the Internet influences security behavior, and our findings related to descriptive norm support the notion that individuals may perceive the Internet to be a public good, there are other factors that should be explored in future research to improve our understanding of differences in what may motivate individuals to protect the Internet versus other devices such as their own computer. For example, the level of self-interest an individual has in the "health" of the Internet likely varies depending on the extent to which they utilize it to connect with others, to transact business, to conduct research, etc. Previous research has shown a connection between personal relationships with vic-

Table 6. Research Contributions and Implications

Domain of Influence	Contribution	Study Outcome
Theoretical	Provides evidence of the importance of psychological ownership as an additional component of PMT in the online security context	Study 1
Theoretical	Provides evidence of the importance of descriptive norm as an additional component of PMT in the online security context	Study 1
Theoretical	Suggests the proximal drivers of intentions to perform security-related behavior vary depending on the target of protection	Study 1
Empirical	Empirical support for the relevance of PMT to broader intentions to protect one's own computer as well as the Internet	Study 1
Practical	Provides practitioners with improved understanding of the factors influencing home computer users' intentions to perform security-related behaviors which can be used to craft policy or social marketing campaigns.	Study 1
Theoretical	Demonstrates that two of the proximal drivers of intentions to perform security-related behaviors, subjective and descriptive norm, can be influenced by message cues	Study 2
Practical	Suggests that the most effective marketing messages in the security behavior context may be those that are promotion focused utilizing an independent self-view	Study 2

tims of disease and charitable contributions (Small and Simonsohn 2008), and self-interest and its effects on social action (Ratner and Miller 2008). Self-interest may be an antecedent to psychological ownership for home users, while factors such as hierarchical position and firm tenure may play a role in organizational contexts. Another factor to consider is the extent to which the individual has developed a role identity related to taking security precautions. An individual who perceives herself to be a person who behaves in secure fashion and feels a greater sense of responsibility for taking security precautions is more likely to do so. Identification with one's role can shift the importance of other social factors on behavior (Charng et al. 1988).

From the perspective of persuasive messaging, although others have alluded to and tested the effects of framing and self view on attitudes and intentions (Aaker and Lee 2001; Lee et al 2000), prior research has not examined how these variables interact to influence norms. Our findings suggest that goal frame and self-view message cues influence subjective and descriptive norms, which, in turn, influence security behavior. Self view is a perception of oneself that can be either situationally activated, as when primed by a message as we have done here, or chronic, as when nurtured by a culture (Heine and Lehman 1997; Kitayama et al. 1997; Lee and Aaker 2001). For example, Western cultures tend to perpetuate an independent self construal, while in Japan the focus is on belonging, and the culture tends to stress an interdependent self construal (Heine and Lehman 1997; Kitayama et al. 1997). To the degree that our findings suggest that situationally primed self-view can influence norms involved in driving security behavior, it is possible that chronic self construal may similarly play a role in security behavior. Prior research shows that situationally activated self-view and chronic self-view produce similar effects (Aaker and Lee 2001; Lee et al. 2000). Therefore, future behavioral security research should involve cross-cultural comparisons.[10]

Managerial Implications

From a practical standpoint, the findings of study 1 are informative in that they suggest possibilities for segmenting consumers for targeted messages and provide more variables to consider when creating advertising campaigns. For example, our findings indicate that consumers differ in the degree to which they feel tied to various objects (e.g., a computer or a network) and that this "closeness" influences their security behavior with regard to that object. Organizations should be aware of this when crafting security messages aimed at employees, and be very specific about which objects the employees are expected to protect through their behaviors (e.g., the physical computer at their office desk, data stored digitally on a thumbdrive or on a network, a laptop, access to a network, etc.) A brief survey might inform management as

[10]Additional opportunities for future research are discussed in Appendix H.

to which objects employees feel a greater sense of psychological ownership toward and, perhaps, those objects should be used in security messages most frequently to encourage appropriate security behavior. Furthermore, if the data reveal that individuals do not experience a sense of ownership toward important organizational assets, managers can take appropriate action to amplify the personal connection to the object.

The results of study 2 suggest that two of the factors influencing security behavior are malleable via a combination of message cues. Our findings reveal that an effective means of influencing the social norms is to combine an independent self view with a promotion-focused goal frame in a security-related message. Thus, organizations creating awareness training and public awareness campaigns should consider focusing consumers on the benefits to be realized by proper security behavior as opposed to the negative consequences, in combination with focusing on the individual as opposed to the individual as part of a group.

Looking Ahead

In conclusion, recent dialog in the trade press and activity at the strategic policy level (Borrus 2005; Campbell et al. 2003; Garg 2003; GAO 2004; Krebs 2005; NSSC 2003; White House 2009a, 2009b; Symantec 2009) collectively suggest that our dependence on technology has created challenges and opportunities of a critical nature for the continued prosperity of both organizations and individuals. There exists a need for rigorous analyses that can inform individuals, managers, and policy makers about appropriate steps and processes for risk mitigation. The studies reported here represent an early step toward understanding individual motivations and predispositions to security attitude and behavior, as well as how to influence these beliefs. The creation of the conscientious cybercitizen is a complex, daunting task that involves providing education, raising general awareness and concern, changing maladaptive behaviors, and changing perceptions that have long been held by many individuals. We hope that this paper serves as a catalyst for additional researchers to begin exploration into this area.

References

Aaker, J. L., and Lee, A. Y. 2001. "'I' Seek Pleasures and 'We' Avoid Pains: The Role of Self-Regulatory Goals in Information Processing and Persuasion," *Journal of Consumer Research* (28:1), pp. 33-50.

Agarwal, R., and Prasad, J. 1997. "The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies," *Decision Sciences* (28:3), pp. 557-582.

Anderson, N. H. 1981. *Foundations of Information Integration Theory*, San Diego: Academic Press.

Astrom, A. N., and Rise, J. 2001. "Young Adults' Intention to Eat Healthy Food: Extending the Theory of Planned Behavior," *Psychology and Health* (16), pp. 223-237.

Ajzen, I. 1988. *Attitudes, Personality and Behavior*, Chicago: The Dorsey Press.

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

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

Andreoni, J. 1995. "Warm-Glow Versus Cold-Prickle: The Effects of Positive and Negative Framing on Cooperation in Experiments," *Quarterly Journal of Economics* (CX:1), pp. 1-21.

Armitage, C. J., and Conner, M. 2001. "Efficacy of the Theory of Planned Behavior: A Meta-Analytic Review," *British Journal of Social Psychology* (40), pp. 471-499.

Armstrong, J. S., and Overton, T. S. 1977. "Estimating Nonresponse Bias in Mail Surveys," *Journal of Marketing Research* (14:3), pp. 396-402.

Arthur, D., and Quester, P. 2004. "Who's Afraid of That Ad? Applying Segmentation to the Protection Motivation Model," *Psychology and Marketing* (21:9), pp. 671-696.

Baroudi, J. J., and Orlikowski, W. J. 1989. "The Problem of Statistical Power in MIS Research," *MIS Quarterly* (13:1), pp. 87-106.

Benbasat, I., and Zmud, R. W. 1999. "Empirical Research in Information Systems: The Practice of Relevance," *MIS Quarterly* (23:1), pp. 3-16.

Block, L. G., and Keller, P. A. 1995. "When to Accentuate the Negative: The Effects of Perceived Efficacy and Message Framing on Intentions to Perform Health-Related Behavior," *Journal of Marketing Research* (32:2), pp. 192-204.

Borrus, A. 2005. "Invasion of the Stock Hackers," *Business Week Online*, November 3 (available online at http://seclists.org/isn/2005/Nov/8).

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18), pp. 151-164.

Brewer, M. B., and Kramer, R. M. 1986. "Choice Behavior in Social Dilemmas: Effects of Social Identity, Group Size, and Decision Framing," *Journal of Personality and Social Psychology* (50), pp. 543-549.

Brown, S. A., and Venkatesh, V. 2005. "Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle," *MIS Quarterly* (29:3), pp. 399-426.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3) pp. 523-548.

Burnkrant, R. E., and Cousineau, A. 1975. "Informational and Normative Social Influence on Buyer Behavior," *Journal of Consumer Research* (2:3), pp. 206-215.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security* (11), pp. 431-448.

Charng, H., Piliavin, J. A., and Callero, P. L. 1988. "Role Identity and Reasoned Action in the Prediction of Repeated Behavior," *Social Psychology Quarterly* (51:4), pp. 303-317.

Chestnut, R. 2004. "E-Commerce Safety Guide." Available online at https://www.paypalobjects.com/WEBSCR-610-20100216-1/en_US/pdf/PayPal_Safety.pdf, accessed on April 3, 2008).

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

Conner, M., and McMillan, B. 1999. "Interaction Effects in the Theory of Planned Behavior: Studying Cannabis Use," *British Journal of Social Psychology* (38), pp. 195-222.

Culnan, M. J. 2004. "Bentley Survey on Consumers and Information Security: Summary of Findings," unpublished paper, Bentley College (available online at http://www.bentley.edu/events/iscw2004/survey_findings.pdf; accessed March 15, 2010).

Culnan, M. J., Foxman, E. R., and Ray, A. W. 2008. "Why IT Executives Should Help Employees Secure Their Home Computers," *MIS Quarterly Executive* (7:1), pp. 49-56.

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

Day, J. C., Janus, A., and Davis, J. 2003. "Computer and Internet Use in the United States: October," U. S. Department of Commerce, Economics and Statistics Administration, U.S. Census Bureau (available online at http://purl.access.gpo.gov/GPO/LPS3637).

DHS. 2003. "National Strategy to Secure Cyberspace," U. S. Department of Homeland Security (available online at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf).

Dipboye, R. L. 1977. "A Critical Review of Korman's Self-Consistency Theory of Work Motivation and Occupational Choice," *Organizational Behavior and Human Performance* (18), pp. 108-126.

Dittmar, H. 1992. *The Social Psychology of Material Possessions: To Have is to Be*, New York: St. Martin's Press.

Dodge, R. C., Carver, C., and Ferguson, A. J. 2007. "Phishing for User Security Awareness," *Computers and Security* (26:1), pp. 73-80.

Dutta-Bergman, M. J. 2004. "The Impact of Completeness and Web Use Motivation on the Credibility of e-Health Information," *Journal of Communication* (54:2), pp. 253-270.

Dyne, L., and Pierce, J. 2004. "Psychological Ownership and Feelings of Possession: Three Field Studies Predicting Employee Attitudes and Organizational Citizenship Behavior," *Journal of Organizational Behavior* (25), pp. 439-459.

Ellen, P. S., and Wiener, J. L. 1991. "The Role of Perceived Consumer Effectiveness in Motivating," *Journal of Public Policy & Marketing* (10:2), pp. 102-117.

Federal Trade Commission. 2002. "FTC Facts for Consumers: Safe at Any Speed, How to Stay Safe Online If You Use High Speed Internet Access" (available online at http://www.otecwb.com/safeonline.pdf; accessed on April 3, 2008).

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

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

Frey, B., and Meier, S. 2004. "Pro-Social Behavior in a Natural Setting," *Journal of Economic Behavior & Organization* (54), pp. 65-88.

Furby, L. 1978. "Possession in Humans: An Exploratory Study of its Meaning and Motivation," *Social Behavior and Personality* (6), pp. 49-65.

Furnell, S. M., Bryant, P., and Phippen, A. D. 2007. "Assessing the Security Perceptions of Personal Internet Users," *Computers and Security* (26), pp. 410-417.

Garg, A. 2003. "What Does an Information Security Breach Really Cost? Evidence and Implications," *Information Strategy: The Executive's Journal* (19:4), pp. 21-25.

GAO. 2004. "Technology Assessment: Cybersecurity for Critical Infrastructure Protection," *GAO Reports*, United States General Accounting Office (available online at http://www.gao.gov/new.items/d04321.pdf).

Gordon, G. 2006. "Low Cost Internet for the Masses," *Sunday Times (South Africa),* Economy, Business and Finance Section, p. 17.

Gross, G. 2007. "Groups Raise Concerns About Cybersecurity Standards," *PC World*, April 25.

Hamilton, R. W., and Biehal, G. 2005. "Achieving Your Goals or Protecting Your Future? The Effects of Self-View on Goals and Choices," *Journal of Consumer Research* (35:2), pp. 277-283.

Heffner, R. R., Kurani, K. S., and Turrentine, T. S. 2005. "Effects of Vehicle Image in Gasoline-Hybrid Electric Vehicles," paper presented at the 21st Worldwide Battery, Hybrid, and Fuel Cell Electric Vehicle Symposium and Exhibition (EVS-21), Monaco, April 2-6.

Heine, S. J., and Lehman, D. R. 1997. "The Cultural Construction of Self-Enhancement: An Examination of Group-Serving Biases," *Journal of Personality and Social Psychology* (72:6), pp. 1268-1283.

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

Higgins, E. T. 1997. "Beyond Pleasure and Pain," *American Psychologist* (52:12), pp. 1280-1301.

Ho, R. 1998. "The Intention to Give Up Smoking: Disease Versus Social Dimensions," *Journal of Social Psychology* (138:3), pp. 368-380.

Isaacs, S. 1933. *Social Development in Young Children*, London: Routledge and Kegan Paul.

Jacoby, J., Morrin, M., Jaccard, J., Gurhan, Z., Kuss, A., and Maheswaran, D. 2002. "Mapping Attitude Formation as a Function of Information Input: Online Processing Models of Attitude Formation," *Journal of Consumer Psychology* (12:1), pp. 21-34.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 548-566.

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* (23:3), pp. 183-213.

Keser, C., and van Winden, F. 2000. "Conditional Cooperation and Voluntary Contributions to Public Goods," *Scandinavian Journal of Economics* (102:1), pp. 23-39.

Kitayama, S., Markus, H. R., Matsumoto, H., and Norasakkunkit, V. 1997. "Individual and Collective Processes in the Construction of the Self: Self-Enhancement in the United States and Self-Criticism in Japan." *Journal of Personality and Social Psychology* (72:6), pp. 1245-1267.

Korman, A. H. 1970. "Toward a Hypothesis of Work Behavior," *Journal of Applied Psychology* (54), pp. 31-41.

Krebs, B. 2005. "Hacking Home PCs Fueling Rapid Growth in Online Fraud," *Washington Post*, Technology Section, Special Reports, Cyber-Security, September 19.

LaRose, R., Rifon, N. J., and Enbody, R. 2008. "Promoting Personal Responsibility for Internet Safety," *Communications of the ACM* (51:3), pp. 71-76.

Lazarus, R. S. 1991. "Progress on a Cognitive–Motivational–Relational Theory of Emotion," *American Psychologist* (46:8), pp. 819-834.

Leach, J. 2003. "Improving User Security Behavior," *Computers and Security* (22:8), pp. 685-693.

Lee, A. Y., and Aaker, J. L. 2004. "Bringing the Frame into Focus: The Influence of Regulatory Fit on Processing Fluency and Persuasion," *Journal of Personality and Social Psychology* (86:2), pp. 205-218.

Lee, A. Y., Aaker, J. L., and Gardner, W. L. 2000. "The Pleasures and Pains of Distinct Self-Construals: The Role of Interdependence in Regulatory Focus," *Journal of Personality and Social Psychology* (78), pp. 1122-1134.

Lee, Y., and Kozar, K. A. 2005. "Investigating Factors Affecting the Adoption of Anti-Spyware Systems," *Communications of the ACM* (48:8), pp. 72-77.

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

Levin, I. P., Schneider, S. L., and Gaeth, G. J. 1998. "All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects," *Organizational Behavior and Human Decision Processes* (76:2), pp. 149-188.

Levy, S. J. 1959. "Symbols for Sale," *Harvard Business Review* (37), pp. 117-124.

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

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

Maheswaran, D., and Meyers-Levy, J. 1990. "The Influence of Message Framing and Issue Involvement," *Journal of Marketing Research* (27:3), pp. 361-368.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale and the Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Mazen, A., Graf, L., Kellogg, C., and Hemmasi, M. 1987. "Statistical Power in Contemporary Management Research," *Academy of Management Journal* (30:2), pp. 369-380.

McCracken, G. 1986. "Culture and Consumption: A Theoretical Account of the Structure and Movement of the Cultural Meaning of Consumer Goods," *Journal of Consumer Research* (13), pp. 71-84.

Mingers, J. 2001. "Combining IS Research Methods: Towards a Pluralist Methodology," *Information Systems Research* (12:3), pp. 240-259.

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

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18), pp. 126-139.

NCSA. 2007. "Eight Cyber Security Practices to Stay Safe Online," National Cyber Security Alliance (available online at http://www.staysafeonline.info/practices/index.html; accessed on March 26, 2008).

NIH. 2007. "NIH IT Security Policy Guidelines," Center for Information Technology, National Institutes of Health (available online at http://www.cit.nih.gov/security.html; accessed on March 26, 2008).

Noyes, A. 2007. "Biggest Threat to Internet Could Be a Massive Virtual Blackout," *National Journal's Technology Daily*, April 5 (available online at http://www.govexec.com/story_page_pf.cfm?articleid=36543&printerfriendlyvers=1; accessed on February 25, 2008).

Nunnally, J. C. 1967. *Psychometric Theory*, New York: McGraw-Hill.

Obermiller, C. 1995. "The Baby Is Sick/The Baby Is Well: A Test of the Environmental Communication Appeals," *Journal of Advertising* (24:2), pp. 55-71.

Pahnila, S., Siponen, M., and Mahomood, A. 2007. "Employees' Behavior Towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, January 3-6, Los Alamitos, CA: IEEE Computer Society Press.

Pavlou, P. A., and Fygenson, M. 2006. "Understanding and Prediction Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly* (30:1), pp. 115-143.

Pechmann, C., Zhao, G., Goldberg, M., and Reibling, E. 2003. "What to Convey in Antismoking Advertisements for Adolescents: The Use of Protection Motivation Theory to Identify Effective Message Themes," *Journal of Marketing* (67:2), pp. 1-18.

Pierce, J., Kostova, T., and Dirks, K. T. 2001. "Toward a Theory of Psychological Ownership in Organizations," *Academy of Management Review* (26:2), pp. 298-311.

Pierce, J., Kostova, T., and Dirks, K. T. 2003. "The State of Psychological Ownership: Integrating and Extending a Century of Research," *Review of General Psychology* (7:1), pp. 84-107.

Plouffe, C. R., Hulland, J. S., and Vandenbosch, M. 2001. "Research Report: Richness Versus Parsimony in Modeling Technology Adoption Decisions—Understanding Merchant Adoption of a Smart-Card Based Payment System," *Information Systems Research (*12:2), pp. 208-223.

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

Ratner, R. K., and Miller, D. T. 2008. "The Norm of Self-Interest and its Effects on Social Actions," *Journal of Personality and Social Psychology* (81:1), pp. 5-16.

Rhee, H., Rhu, Y., and Kim, C. 2005. "I Am Fine But You Are Not: Optimistic Bias and Illusion of Control on Information Security," in *Proceedings of the 26th International Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, December 11-14, pp. 381-394.

Rifon, N., Quilliam, E. T., and LaRose, R. 2005. "Consumer Perceptions of Online Safety," paper presented at the International Communication Association, Communication and Technology Division, New York, NY, May 27 (available online at https://www.msu.edu/~isafety/papers/ICApanelfg.htm).

Rippetoe, P. A., and Rogers, R. W. 1987. "Effects of Components of a Protection Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat," *Journal of Personality and Social Psychology*, (52), pp. 596-604.

Rivis, A., and Sheeran, P. 2003a. "Descriptive Norms as an Additional Predictor in the Theory of Planned Behaviour: A Meta-Analysis," *Current Psychology* (22:3), pp. 218-233.

Rivis, A., and Sheeran, P. 2003b. "Social Influences and the Theory of Planned Behavior: Evidence for a Direct Relationship Between Prototypes and Young People's Exercise Behavior," *Psychology and Health* (18), pp. 567-583.

Rivis, A., and Sheeran, P. 2006. "Augmenting the Theory of Planned Behavior with the Prototype/Willingness Model: Predictive Validity of Actor Versus Abstainor Prototypes for Adolescents' Health-Protective and Health-Risk Intentions," *British Journal of Health Psychology* (11:3), pp. 483-500.

Rochberg-Halton, E. 1980. "Cultural Signs and Urban Adaptation: The Meaning of Cherished Household Possessions," unpublished doctoral dissertation, University of Chicago.

Rogelberg, S. G., and Stanton, J. M. 2007. "Introduction: Understanding and Dealing with Organizational Survey Nonresponse," *Organizational Research Methods* (10:2), pp. 195-209.

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

Rosemann, M., and Vessey, I. 2008. "Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks," *MIS Quarterly* (32:1), pp. 1-22.

Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'Weakest Link'—A Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3), pp. 122-131.

Senn, J. 1998. "The Challenge of Relating IS Research to Practice," *Information Resources Management Journal* (11:1), pp. 23-28.

Schulman, Ronca, & Bucuvalas, Inc. 2007. "Michigan State University Safety Survey Technical Report." Accessed online at http://www.msu.edu/~isafety/finalreport.pdf, accessed on March 24, 2008).

Sheeran, P. 2002. "Intention-Behaviour Relations: A Conceptual and Empirical Review," in *European Review of Social Psychology* (12), W. Stroebe and M. Hewstone (eds.), London: Wiley, pp. 1-36.

Sheeran, P., and Taylor, S. 1997. "Predicting Intentions to Use Condoms: Meta-Analysis and Comparison of the Theories of Reasoned Action and Planned Behavior," *Journal of Applied Social Psychology* (29), pp. 1624-1675.

Shiv, B., Britton, J. A. E., and Payne, J. W. 2004. "Does Elaboration Increase or Decrease the Effectiveness of Negatively Versus Positively Framed Messages?," *Journal of Consumer Research* (31:1), pp. 199-208.

Sigall, H., and Mills, J. 1998. "Measures of Independent Variables and Mediators Are Useful in Social Psychology Experiments: But Are They Essential?," *Personality and Social Psychology Review* (2:3), pp. 218-226.

Singelis, T. M. 1994. "The Measurement of Independent and Interdependent Self-Construals," *Personality and Social Psychology Bulletin* (20:5), pp. 580-591.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Sivo, S. A., Saunders, C., Chang, Q., and Jiang, J. J. 2006. "How Low Should You Go? Low Response Rates and the Validity of Inference in IS Questionnaire Research," *Journal of the Association of Information Systems* (7:6), pp. 351-414.

Small, D. A., and Simonsohn, U. 2008. "Friends of Victims: Personal Experience and Prosocial Behavior," *Journal of Consumer Research* (35), pp. 532-542.

Stanton, J. M., and Stam, K. R. 2006. "An Introduction to Information Protection and Employee Behavior," Chapter 1 in *The Visible Employee*, Medford, NJ: Information Today, Inc.

Stanton, J. M., Stam, K. R., Mastrangelo, P. M., and Jolton, J. A. 2005. "Analysis of End User Security Behaviors," *Computers & Security* (24), pp. 124-133.

Stasson, M., and Fishbein, M. 1990. "The Relation Between Perceived Risk and Preventive Action: A Within-Subject Analysis of Perceived Driving Risk and Intentions to Wear Seatbelts," *Journal of Applied Social Psychology* (20:19), pp. 1541-5157.

Straub, D. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Symantec. 2009. "Symantec Internet Security Threat Report: Trends for 2008," Symantec Corporation, Cupertino, CA, April (available online at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet

_security_threat_report_xiv_04-2009.en-us.pdf;accesssed March 15, 2010).

Takemura, K. 1994. "Influence of Elaboration on the Framing of Decision," *Journal of Psychology* (128), pp. 33-39.

Tanner, J., Hunt, J. B., and Eppright, D. R. 1991. "The Protection Motivation Model: A Normative Model of Fear Appeals," *Journal of Marketing* (55), pp. 36-45.

Taylor, S., and Todd, P. 1995. "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research* (6:2), pp. 144-176.

Trafimow, D., and Fishbein, M. 1994. "The Importance of Risk in Determining the Extent to Which Attitudes Affect Intentions to Wear Seat Belts," *Journal of Applied Social Psychology* (24:1), pp. 1-11.

Tversky, A., and Kahneman, D. 1981. "The Framing of Decisions and the Psychology of Choice," *Science* (211), pp. 453-458.

Tversky, A., and Kahneman, D. 1984. "Choice, Values and Frames," *American Psychologist* (39:4), pp. 341-350.

Tversky, A., and Kahneman, D. 1986. "Rational Choice and the Framing of Decisions," *Journal of Business* (59:4), pp. S251-S278.

Van Dijk, E., and Wilke, H. 1997. "Is It Mine or Is It Ours? Framing Property Rights and Decision Making in Social Dilemmas," *Organizational Behavior and Human Decision Processes* (71:2), pp. 195-209.

Venkatesh, V., and Davis, F. D. 2000. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science* (45:2), pp. 186-203.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-278.

Vroom, C., and Von Solms, R. 2004. "Towards Information Security Behavioral Compliance," *Computers & Security* (23), pp. 191-198.

Walker, R. W. 2007. "Infrastructure Security on GAO's High-Risk List," *Government Computer News*, January 31 (available online at http://gcn.com/articles/2007/01/31/infrastructure-security-on-gaos-highrisk-list.aspx).

Wang, X. T. 1996. "Evolutionary Hypotheses of Risk-Sensitive Choice: Age Differences and Perspective Change," *Ethology and Sociobiology* (17), pp. 1-14.

Webb, T. L., and Sheeran, P. 2006. "Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence," *Psychological Bulletin* (132:2), pp. 249-268.

Weirich, D., and Sasse, M. A. 2001. "Pretty Good Persuasion: A First Step Towards Effective Password Security in the Real World," in *Proceedings of the 2001 Workshop on New Security Paradigms*, Cloudcroft, NM, September 10-13, pp. 137-143.

White, R. W. 1959. "Motivation Reconsidered: The Concept of Competence," *Psychological Review* (66), pp. 297-330.

White House. 2009a. "The American Recovery and Reinvestment Act" (available online at http://www.whitehouse.gov/recovery/about/, accessed on August 18, 2009).

White House. 2009b. "Cyberspace Policy Review" (available online at http://www.whitehouse.gov/assets/documents/ Cyber space_Policy_Review_final.pdf; accessed on June 30, 2009).

Williams, L. J., Edwards, J. R., and Vandenberg, R. J. 2003. "Recent Advances in Causal Modeling Methods for Organizational and Management Research," *Journal of Management* (29:6). 2003, pp. 903-936.

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

Woon, I. M. Y., Tan, G. W., and Low, R. T. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in *Proceedings of the 26th International Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross, Las Vegas, December 11-14, pp. 367-380.

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

Zajonc, R. B. 1968. "Attitudinal Effects of Mere Exposure," *Journal of Personality and Social Psychology Monograph Supplement* (9:2), pp. 1-27.

About the Authors

Catherine L. Anderson is a doctoral candidate in the Information Systems Program in the Decision, Operations, and Information Technologies Department of the Robert H. Smith School of Business at the University of Maryland. Cathy's research interests broadly involve understanding how organizations and individuals respond to vulnerabilities introduced by increased dependence on technology. Her current work is in behavioral aspects of security, consumer health information privacy concerns, and technology reliability. She has presented her research at the International Conference on Information Systems, the Academy of Management Conference, and INFORMS, and her work is currently under review at several major information systems and management journals. She was a finalist in the Organization Science Dissertation Proposal Competition in 2008. Her dissertation was partially funded by a dissertation grant from the Decision, Risk and Management Sciences Program of the National Science Foundation. Prior to returning to school for her doctorate, Cathy was a consultant for 10 years with Accenture.

Ritu Agarwal is a professor and the Robert H. Smith Dean's Chair of Information Systems at the Robert H. Smith School of Business, University of Maryland, College Park. She is also the founder and director of the Center for Health Information and Decision Systems at the Smith School. Ritu has published over 75 papers on information technology management topics in journals such as *Information Systems Research*, *MIS Quarterly*, *Management Science*, *Communications of the ACM*, *Journal of Management Information Systems*, *Decision Sciences*, *IEEE Transactions*, and *Decision Support Systems*. She has served as a senior editor for *MIS Quarterly* and *Information Systems Research*. Her current research is focused on the use of IT in healthcare settings, information privacy and security, social networks and their impacts, and consumer behavior in technology-mediated settings.