An Extended Perspective on Individual Security Behaviors

Article *in* ACM SIGMIS Database · November 2014

DOI: 10.1145/2691517.2691521

2 authors:

Robert E. Crossler
Washington State University
34 PUBLICATIONS **825** CITATIONS

SEE PROFILE

France Belanger
Virginia Polytechnic Institute and State University
123 PUBLICATIONS **5,580** CITATIONS

SEE PROFILE

An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument

Robert Crossler
Mississippi State University

France Bélanger
Virginia Tech

An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument

Robert Crossler
Mississippi State University

France Bélanger
Virginia Tech

Acknowledgment

We would like to thank the participants in The 2010 Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13, for their helpful feedback on an earlier version of this paper.

Abstract

Security threats regularly affect users of home computers. As such, it is important to understand the practices of users for protecting their computers and networks, and to identify determinants of these practices. Several recent studies utilize Protection Motivation Theory (PMT) to explore these practices. However, these studies focus on one specific security protection behavior or on intentions to use a generic measure of security protection tools or techniques (practices). In contrast, this study empirically tests the effectiveness of PMT to explain a newly developed measure for collectively capturing several individual security practices. The results show that PMT explains an important portion of the variance in the unified security practices measure, and demonstrates the importance of explaining individual security practices as a whole as opposed to one particular behavior individually. Implications of the study for research and practice are discussed.

Keywords: Information Security, Security Practices, Protection Motivation Theory, Home User

ACM Categories: K.6.5, K.4.2.

General Terms: Measurement, Security, Theory.

Introduction

Security threats compromise a significant number of personal computers, with 30 percent of computers in the United States infected with malware (PandaLabs 2012). These security threats result in a number of computers having “bots” installed on them, allowing the computers to be used at the whim of the hackers who control them (Ricadela 2007). These bots are multi-purpose in nature, in that they give full administrative privileges of the victim’s machine to the criminal running the malware, which gives the criminal the ability to use the victim’s computer to conduct distributed denial of service attacks on other computers, to distribute spam across the Internet, to open backdoors to one’s computer, or to install software to capture keystrokes on the victim’s machine (Damballa 2011). These malware infections may ultimately result in financial loss for companies or in identify theft issues for individuals (Ahamad et al. 2008). Individuals are increasingly the targets of these attacks, resulting in significant financial costs for individuals as well as compromising the safety of the infrastructure of the Internet (Anderson and Agarwal 2010). One sophisticated way that hackers are getting malware (viruses, worms, etc.) onto individuals’ computers is by taking advantage of social networking sites. For example, a Facebook.com user

could share a link to a YouTube video with a number of friends, a video that may require the user to download an "update" to view it. In downloading the "update", the user is in fact downloading malware that infects the computer being used with a bot, making it part of a larger botnet (Ahamad et al. 2008).

As stated, compromised home computers can become part of botnets, groups of computers under the remote control of an individual, posing a significant number of problems for home users, companies, and governments. It is estimated that the top botnet alone consists of 2.2 million bot computers, which are used to distribute spam and malware every day. When the other top 20 bot networks and other malware infections are included, over 7.5 million computers are infected (Kindsight 2012). From a government's perspective, the use of botnets from compromised computers is even more troublesome. Recent military engagements have illustrated the importance that cyber warfare plays in a successful campaign. The proliferation of botnet-affected computers provide a readily available set of resources for mounting a cyber-warfare campaign against a country (Ahamad et al. 2008). The significant problem posed by botnets is amplified when one considers that the Conficker worm alone provides a larger cloud computing network for criminals than those offered legitimately to corporations by companies such as Google and Amazon (Mullins 2010).

Human error is an important source of security threats (Im and Baskerville 2005), which cannot be controlled by technical solutions alone (Siponen and Oinas-Kukkonen 2007). As a result, it is important for individuals to secure their personal computers and networks. Table 1 presents a number of volitional practices these individuals can take to do so.

Table 1. Individual Volitional Security Practices

Practice	Source
Anti-Malware Software Usage	(Johnston and Warkentin 2010)
Authentication Tools	(Zviran and Erlich 2006; Zviran and Haga 1999)
Operation System and Programmatic Security Features	(Furnell et al. 2006)
Privacy Protection Tools	(Furnell et al. 2007)
Protective Technologies	(Dinev and Hu 2007)
Vulnerability Management	(Al-Ayed et al. 2005)
Wireless Security Management	(Woon et al. 2005)

This study focuses on determining the factors that influence the volitional security practices home users should perform to secure their systems to avoid malicious IT threats on their own computers and networks. Researchers and professionals agree that people are often the weakest link in security (Crossler et al. 2013), but until recently (Anderson and Agarwal 2010; Boss et al. 2009; Guo et al. 2011; Herath and Rao 2009a; Herath and Rao 2009b; Johnston and Warkentin 2010; Kumar et al. 2008; Workman et al. 2008) few studies have tried to understand the human component of a secure information system (Cannoy et al. 2006; Choobineh et al. 2007; Dhillon and Backhouse 2001).

A number of theories have been explored to explain security behaviors, including organizational control (e.g. Boss et al. 2009), the theory of planned behavior (e.g. Dinev and Hu 2007), rational choice theory (e.g. Aytes and Connolly 2004), general deterrence theory (e.g. Herath and Rao 2009b), and protection motivation theory (e.g. Anderson and Agarwal 2010; Johnston and Warkentin 2010). Several of these studies have used an adaptation of Protection Motivation Theory (PMT) to explain differences in security practices. To date, these studies have not empirically tested the theories proposed (Liang and Xue 2009), or have tested the theory with only one measure such as intention to use one particular security tool like anti-spyware (e.g., Johnston and Warkentin 2010; Kumar et al. 2008), intentions to generically perform security related behavior (e.g., Anderson and Agarwal 2010), or intentions to comply with security policies (e.g., Herath and Rao 2009b). However, as mentioned above, securing a computer is about performing a number of different practices, not one in particular. It has been shown that theories that can explain a wide arching set of behaviors as opposed to one individual behavior provide a more holistic understanding of why people perform these behaviors (Hanisch et al. 1998). For example, if an individual regularly updates his anti-virus software but has no firewall and extremely poor passwords, the individual would be ranked as high security if a researcher is only looking at anti-virus software, whereas in reality the overall security of his systems is low.

The goal of this paper is to expand the understanding of PMT by empirically testing it using a unified measure of security related practices (e.g. anti-virus software usage, anti-spyware software usage, properly securing wireless networks, software patches and updates, data backup, user account setups, screen saver usage, password behaviors, credit card storage online, and email link clicking behavior) rather

than the individual measures previous studies utilized. The results of the test of this unified measure of security practices demonstrate its importance to future IS research. By demonstrating that PMT explains a unified set of security practices, this paper provides empirical evidence that PMT findings can be generalized from individual specific behaviors to a broader set of practices. These findings also shed additional light into the understanding of PMT in the information security context, and provide a useful construct for future information security research. Furthermore, this research utilizes a statistical approach that allows the unified measure of security practices to be collapsed into a single score for each individual respondent. Such an approach provides for a statistical way to compare different individuals on their overall performance on a set of security practices.

The paper is organized as follows: the next section defines unified security practices, which is followed by the theoretical foundations of the research. The subsequent section presents the methodology that was utilized to develop and validate the instruments used in this research and to test the research model. The results are then presented, followed by a discussion of the key findings. Finally, the paper concludes with a summary of the contributions of this research along with directions for future research.

Background Literature

Existing IS research treats security practices as one behavior in particular or computer behaviors in a general sense (Anderson and Agarwal 2006; Anderson and Agarwal 2010; Aytes and Connolly 2004; Boss et al. 2009; Herath and Rao 2009b; Johnston and Warkentin 2010; Kumar et al. 2008; Workman et al. 2008). Given the early nature of this research, there appears to be little consistency in the practices studied. In addition, a very small subset of this literature studies the protective practices home users employ, as opposed to users within an organizational setting. Yet, research in this area is particularly important not just for the sake of the home users but for corporations as well (Culnan et al. 2008).

The state of research involving individual security practices is consistent with the overall state of security research in the field of IS in general. A review of 82 papers on security in the top IS journals from 1996 to 2005 found that research in information systems security is very fragmented with very few papers testing research hypotheses, and no framework emerging to explain security research (Cannoy et al. 2006). Cannoy and colleagues also show that there has been no consistency in the variables used to explain security, and that very few studies include major constructs and their relationships; rather, they focus on narrow topics or clarify the details of a technical system.

An investigation of recent work in this domain provides support for Cannoy et al.'s claim that no dependent variable has emerged as an agreed upon measure for this stream of research. For example, one study focused on password "hygiene" (Stanton et al. 2005); another on behavioral intentions to use protective technologies (Dinev and Hu 2007) or more particularly anti-spyware software (Johnston and Warkentin 2010; Kumar et al. 2008); and yet another on end users' understanding of the security features built into often used operating systems and programs (Furnell et al. 2006). One study found that professionals were not receiving security training, and those that did, viewed it as something that they only needed to do once. More importantly, when these same individuals reviewed their security practices at home, weaknesses were found in almost all areas (Kim 2005). Finally, when theories look at a specific task being performed, it is difficult to generalize the findings to the numerous security tasks that individuals need to be performing to protect their computer. To address this, other studies have focused on security practices in general but do not explore the specific tasks performed (Anderson and Agarwal 2010; Boss et al. 2009; Herath and Rao 2009b; Workman et al. 2008). Such an approach relies more on the perception of the general standard a user thinks she is performing up to, and does not specifically measure what she is doing or believe she is doing.

Unified Security Practices (USP)

As previously discussed, measuring only one security behavior does not adequately reflect the necessary measures that people should take when securing their computers and networks. According to Symantec, consumers on the Internet should use and update antivirus software regularly, use a bidirectional firewall, use browser level protection from web-based attacks, as well as use care and knowledge when visiting websites (Zviran and Haga 1999).

Similar recommendations exist for corporations to utilize a portfolio of varying components to protect themselves from a number of threats (Kumar et al. 2008) or in other words to practice defense in depth. Defense in depth is defined by the NSA as "a strategy for achieving Information Assurance" through a "robust and integrated set of information assurance measures and actions" at the personnel, technical, and operational levels (Guo et al. 2011). The NSA considers the personnel level to include tasks revolving around the people in the organization. These security measures involve training and awareness, policies and procedures, and physical

security. The technical level includes insuring the right solutions are purchased and deployed to protect from information security threats. The operational level includes making sure the day-to-day security activities are performed. This includes dealing with system backup and recovery, key management, and keeping security policies up to date. In order for individuals to protect their computers from attack, they also must apply several layers of protection similarly to the recommendations of the NSA. For example, at the personal level, they must make sure they are knowledgeable about making decisions related to links to click on and websites to visit; at the technical level, they should be using technical solutions such as anti-virus software and firewalls; at the operational level, they should be making sure their data is backed up and can be recovered if necessary. Consistent with these recommendations researchers should recognize the need for a unified measure of security practices in information security research.

Theoretical Foundations

Protection Motivation Theory (PMT) has proven to be a useful theoretical foundation for understanding the process that individuals go through in deciding which security behaviors to exercise. When a potential security threat is discovered, individuals go through a process of first recognizing they are threatened by malicious technology, then coping with the malicious threat and deciding whether they are satisfied with the mitigation or removal of the threat based on their coping process (Liang and Xue 2009). PMT supports the process that begins with receiving information (sources of information), which leads to an evaluation of the information by the person receiving it (cognitive mediating process), and finally to the person using this information to take some action (coping mode). The sources of information include environmental and intrapersonal sources. Environmental sources of information include verbal persuasion and observational learning. Intrapersonal sources include personality aspects and feedback from prior experience, including experiences associated with performing the behavior of interest (Floyd et al. 2000; Maddux and Rogers 1983; Rogers 1975). The cognitive mediating process includes two distinct processes: the threat appraisal process and the coping appraisal process. The outcome of the cognitive mediating processes is a decision to apply the applicable adaptive response or the behavior of interest. The two types of coping modes are adaptive coping (to protect the self or others) and maladaptive coping (not to protect the self or others) (Floyd et al. 2000; Maddux and Rogers 1983; Rogers 1975). Figure 1 models this process.

The threat appraisal process involves the user deciding whether he perceives that he is vulnerable to a given threat (perceived vulnerability) and the severity of the threat (perceived severity). The coping appraisal process involves the user deciding whether a protective action is effective at providing protection from the threat (response efficacy), whether he is capable of performing the protective action (self-efficacy) and if it is worth the perceived cost of doing so (perceived cost).

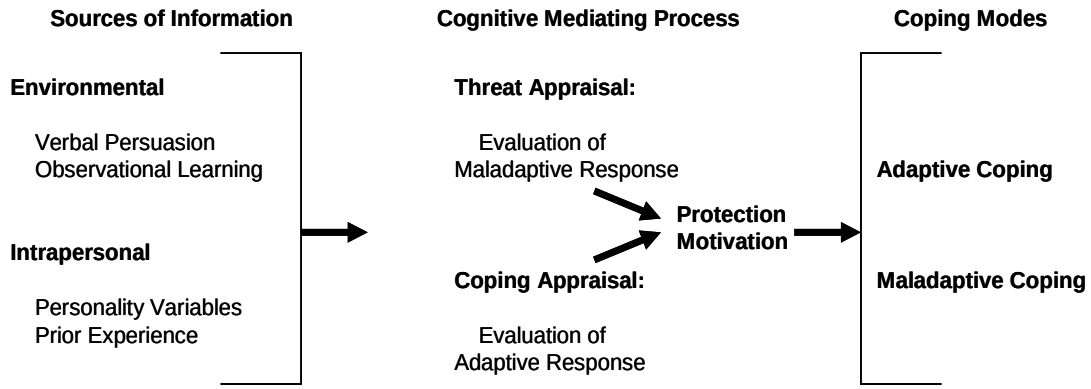

Figure 1. Protection Motivation Theory (Floyd et al. 2000)

A number of researchers explain security practices of individuals by utilizing an adaptation of PMT. In one study, students and employees of a university were surveyed as to their intentions to use anti-spyware software (Johnston and Warkentin 2010). Johnston and Warkentin found that response efficacy, self-efficacy, and social influence positively affect a person's intention to use anti-spyware software. They also found that perceived threat severity negatively affected both response efficacy and self-efficacy, while perceived threat susceptibility did not significantly affect either of the efficacy constructs. An additional study showed that the adoption of anti-malware software was positively affected by perceived severity, perceived vulnerability, response efficacy, self-efficacy, and social influence, and was negatively affected by response cost (Kumar et al. 2008). Another study explored personal computer security behavior intentions as one dependent variable and Internet related behaviors as another (Anderson and Agarwal 2010). Anderson and Agarwal found that the threat appraisal variables, security behavior self-efficacy, and perceived citizen effectiveness affect attitude toward security related behavior, which helped determine whether a person intended to perform security-related behaviors both online and on their personal computer. A further study found that perceived threat severity, response cost, self-efficacy, and response efficacy affect a person's security attitude, which does not affect security policy compliance. The only PMT-based construct that affected security policy compliance in the study is self-efficacy (Herath and Rao 2009b).

Similar to other IS research utilizing PMT (Anderson and Agarwal 2010; Herath and Rao 2009b; Johnston and Warkentin 2010; Kumar et al. 2008), we focus on the adaptive coping response of PMT. This is the behavior that computer users perform to prevent the threat from manifesting itself. The alternative, maladaptive coping, is the individuals' decision not to perform the security practices that protect them from the threat. Thus, following with previous research, investigating the determinants of adaptive coping, or the proactive steps people take to protect themselves from threats, provides the insight necessary to encourage further performance of these protective security tasks. However, unlike previous IS research that has focused on one security practice in particular or the idea of IS security in general, this study investigates a number of practices that in combination provide a greater level of protection from security threats. Figure 2 presents the research model that will be used to test PMT constructs with the unified security practices construct. Although several different adaptations of PMT have been published in the IS literature, we developed the research model for this study by trying to closely mirror the way the theory was used in its originating discipline (Floyd et al. 2000; Maddux and Rogers 1983; Rogers 1975; Rogers et al. 1997). This results in the use of an adaption of PMT that is similar to the work by Lee and Larsen (2008) and Woon and colleagues (2005) where the PMT constructs lead directly to the dependent variable of the security practices of interest. The remainder of the section will provide further details and identify the related hypotheses.

Threat Appraisal

PMT posits that threat appraisal is one determinant that impacts whether a person adopts a given coping response (Floyd et al. 2000). As noted above, threat appraisal is comprised of perceived severity and perceived vulnerability. Perceived severity is defined as an individual's assessment of the severity of the consequences resulting from a threatening security event. Perceived vulnerability is defined as an individual's assessment of the probability of a threatening security event occurring (Kumar et al. 2008).

Perceived Severity. Past research shows that perceived severity positively influences the security practices of individuals. In one study, when investigating the intentions for executives to adopt anti-malware software, perceived severity had a positive relationship with intentions to adopt anti-malware software for all executives studied as well as when executives were separated out into those who were IS experts or not, and those did or did not work in an IT-intensive industry (Kumar et al. 2008). These results are consistent with other studies that found that concern about security threats positively influences security attitudes, which positively affects intentions to perform security behaviors (Anderson and Agarwal 2010). In another study, perceived severity positively influenced security attitude, which did not have a significant relation with intentions to comply with security policies (Herath and Rao 2009b). Another study found that perceived severity positively affected whether or not people properly secured their wireless networks (Woon et al. 2005). Consistent with these studies, it is expected that perceived severity will positively influence Unified Security Practices.

> H1: Perceived severity positively influences volitional Unified Security Practices.

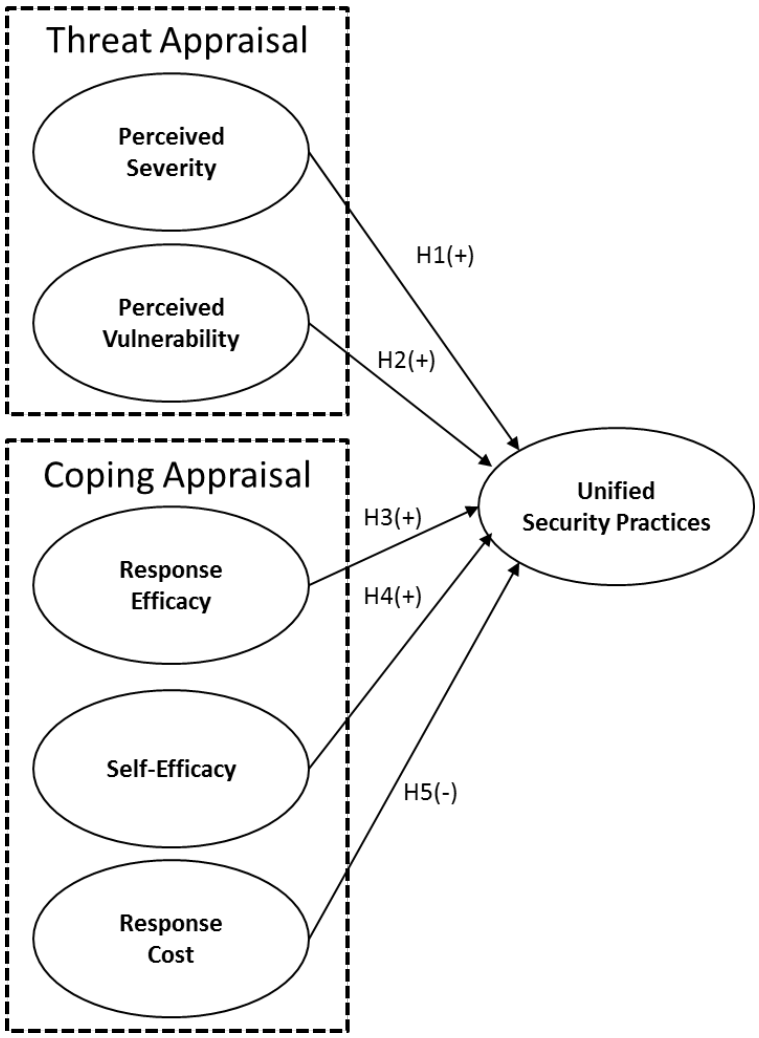

Figure 2. Research Model

Perceived Vulnerability. Perceived vulnerability is regularly hypothesized to have a positive relationship with security practices. However, findings are inconsistent in how perceived vulnerability actually affects these practices. In one study, perceived vulnerability was shown to positively affect intentions to adopt anti-malware software (Kumar et al. 2008). In drilling down to find a more specific understanding of this relationship, it was found that this relationship only held for IS experts and those who worked in IT intensive industries. When explaining whether people will comply with security policies, perceived vulnerability did not have a significant relationship with security attitude (Herath and Rao 2009b). A further study did not find a significant relationship between perceived vulnerability and properly securing wireless networks (Woon et al. 2005). Given the theoretical support from PMT, even with the mixed findings from prior research, it is expected that perceived vulnerability will positively influence individuals' security practices.

H2: Perceived vulnerability positively influences volitional Unified Security Practices.

Coping Appraisal

PMT posits that in addition to threat appraisal, coping appraisal is a determinant of whether a person adopts a given coping response (Floyd et al. 2000). As noted above, coping appraisal is comprised of response efficacy, self-efficacy and response cost. Response efficacy is defined as an individual's confidence that a recommended behavior will prevent or mitigate the threatening security event. Self-efficacy is defined as an individual's confidence in his/her own ability to perform the recommended behavior to prevent or mitigate the threatening security event. Response cost is defined as the cost (e.g. monetary, time,

cognitive) of preventing a threat from manifesting into a successful attack.

Response Efficacy. Response efficacy is a similar measure as outcome expectations, a regularly used IS construct. Outcome expectations represent a "person's estimate that a given behavior will lead to certain outcomes" (Bandura 1977), and it has been found to influence the performance or acceptance of technology (Chung et al. 2002; Compeau et al. 1999; Compeau and Higgins 1995b; Lam and Lee 2006; Venkatesh et al. 2003). PMT research has found similar results using response efficacy to explain performance of security tasks. Response efficacy has a positive relationship with executives' intentions to adopt anti-malware software (Kumar et al. 2008). Interestingly, this relationship only holds for non-IS experts and for those who work in non-IT intensive industries. Further PMT research confirms these findings with response efficacy positively influencing the use of anti-spyware software (Johnston and Warkentin 2010) and properly securing home wireless networks (Woon et al. 2005). Consistent with these studies, other research found that response efficacy positively affected security attitude (Herath and Rao 2009b). Following this previous research, it is expected that response efficacy will positively influence individuals' Unified Security Practices.

H3: Response efficacy positively influences volitional Unified Security Practices.

Self-Efficacy. Self-efficacy was initially conceptualized by Bandura (1977) as "the conviction that one can successfully execute the behavior required to produce outcomes". Since its initial conceptualization, a number of studies have applied the concept of self-efficacy to explain individuals' performance at using computers (Carlson and Grabowski 1992; Compeau et al. 1999; Compeau and Higgins 1995a; Fagan et al. 2003; Fenech 1998; Johnson and Marakas 2000; Lee et al. 2003; Stephens 2005). PMT research has found similar results when relying on self-efficacy to explain performance of security tasks. Self-efficacy has a positive relationship with executives' intentions to adopt anti-malware software (Kumar et al. 2008). Interestingly, and the same as with response efficacy, this relationship only holds for non-IS experts and those who work in non-IT intensive industries. Further studies find a positive relationship between self-efficacy and the use of anti-spyware software (Johnston and Warkentin 2010) as well as properly securing a home wireless network (Woon et al. 2005) and complying with security policies (Herath and Rao 2009b). Similar to these findings, other research found a positive relationship between self-efficacy and security attitudes (Anderson and Agarwal 2010). Therefore, it is expected that self-efficacy will positively influence unified security practices.

H4: Self-efficacy positively influences volitional Unified Security Practices.

Response Cost. PMT posits that as the response cost goes up, the likelihood of performing the adaptive coping response goes down. IS research has found support for these findings with the intentions of executives to adopt anti-malware software being lower when response cost is high (Kumar et al. 2008). These findings hold regardless of IS expertise or the IT intensiveness of an industry the executive works in. Further research supports these findings with response cost negatively influencing whether people properly secure their home wireless network (Woon et al. 2005). These findings are in line with other security research where a security countermeasure will not occur when the cost of responding to a security threat is greater than the damage of the resulting threat (Lee et al. 2002). This is similar to technology adoption literature, which shows that as the cost for using a technology increases, an individual becomes less likely to use the technology (Ghorab 1997; Reardon and Davidson 2007; Wu and Wang 2005). Such findings from previous research suggest that as the cost of invoking a coping response increases, then the likelihood of implementing the response goes down. Following this, it is expected that response cost will be negatively related to performing security tasks.

H5: Response cost negatively influences volitional Unified Security Practices.

Methodology

Figure 2 presented a graphical representation of the hypotheses. Since there is no existing measure of unified security practices, we first discuss the development of the unified security practices (USP) instrument before testing the PMT-based hypotheses.

USP Instrument Development[1]

An investigation of existing security research reveals that few of the measures have gone through an extensive validation process. This is problematic as

[1] We discuss the instrument development in this section. However, for further details on how to conduct the statistical analyses related to the USP instrument, please contact the first author.

Phase	Steps by Churchill	Steps in This Research	Main Results
Phase 1 Conceptual development and initial item generation	1.1 Literature review • Frameworks • Existing measures	1.1 Literature review • Frameworks • Existing measures	• PMT, GDT, need for more behavioral security research • Isolated security practices or generic measures
	1.2 Field interviews • New measures • Insights	1.2 Round 1 expert interviews • Requirement for new measures • Insights on security behaviors	• Need for unified practices • Insights on required practices
	1.3 Focus groups • Nominal group process • New measures	1.3 Round 2 and 3 expert interviews • Saturation on security behaviors • New security behavior measure	• Agreement on required security practices • Preliminary list of unified security practices • Preliminary grouping of practices
Phase 2 Conceptual refinement and item modification	2.1 Sorting procedure • Qualitative assessment of construct validity	2.1 Pre-test with 8 doctoral students • Qualitative assessment of construct validity	• Refinement of item wording
	2.2 Pilot test 1 • Assessment of content validity	2.2 Pilot test 1 with 296 undergraduate students • Assessment of content validity	• Refined list of items for survey
	2.3 Pilot test 2 • Refinement and test of online survey	2.3 Pilot test 2 with 279 citizens • Refinement and test of online survey	• Scale validation – 3 point scale better than 5 point scale for some items
	2.4 Final refinement of items • 15 final measurement items	2.4 Final test of instrument with 81 graduate students • nomological network test	• Unified security practices instrument

Figure 3. Research Process (Adapted from Churchill, 1979)

without evidence of validity there is no assurance that the phenomenon of interest is actually being successfully measured (Straub 1989), and without a standardized dependent variable it is difficult for researchers to cumulate knowledge on what people do to protect themselves from security threats and the factors leading to such practices (Churchill 1979). Therefore, part of our research involves the development and validation of a unified measure of security practices to provide a molar theoretical view of the determinants of a wide-arching set of security practices. Unified Security Practices (USP) are the tasks individuals perform to avoid malicious IT threats on their home computers and networks.

To develop an instrument to measure USP, we follow the procedures recommended by Straub (1989) and Churchill (1979). First, we reviewed existing literature and identified items that were recommended for properly securing home computers and networks. This was followed by further identifying security tasks and proper ways to measure them through interviews of IS

security experts, resulting in an initial instrument. This initial instrument is then refined and tested through a pretest and several pilot tests. Technical validation is performed on additional data collected using the resulting instrument. Finally, we test the newly designed instrument as part of the PMT-based research model hypothesized in this study. Figure 3 summarizes the steps performed in this research and the various samples used.

Initial Instrument Design

The first stage in developing the USP instrument is to identify recommended practices and proper ways to measure them. Initially, the literature was reviewed to identify recommended security tasks and the way that they were measured. Then a panel of seven experts in information security, including representatives from academia, military, and corporations ranging in location from the Southeast to the Northwest of the United States, provided their opinion on necessary protective security practices. Experts were determined to be individuals who trained others in information security, performed research in information security, or were end users with significant training in information security. Each expert participated in three sets of interviews over several months, beginning with an unstructured interview, followed by a semi-structured interview, and ending with a highly structured interview.

The first interview gathered knowledge from the experts on what they thought individual security practices were, as well as the threats from which each practice protects people. They discussed practices they performed that influenced the security of information they had on their computer, or the security of information they had access to from their home computer. Follow up questions provided clarification of the practice performed, as well as more details about threats the expert was protecting himself from by performing the security task. Interestingly, all security practices identified in the literature were mentioned by the experts, except anti-phishing software and encryption. Anti-phishing software might be lesser known or believed to be part of anti-spyware; encryption might not be seen as an end-user security task. These possibilities should be explored in future research.

After the first round of interviews, results were analyzed, looking for agreement on a number of practices, resulting in an initial survey instrument. The second interviews provided clarification for differences between the comments experts provided during round one. For example, some experts gave conflicting advice about certain practices such as whether to write down passwords or not[2]. Clarification was necessary to ensure that consensus was reached on what practices should be performed and why. These interviews also included questions to provide insights into how best to measure the practices identified. Questionnaire items were then refined based on the outcomes of the second interviews. If experts did not agree on whether an item should be included, it was removed from further analysis. Experts reviewed the newly designed questionnaire in the third interviews for any unclear or ambiguous items. The questionnaire was adjusted again based on feedback given during round three.

Pretest and Pilot Test

A group of eight doctoral students pre-tested the initial instrument. They read the instrument and provided feedback on questions that were unclear or ambiguous. Their feedback led to adjustments in the instrument. Then, in order to determine the optimal USP scale, 60 participants from two graduate business classes were administered the USP instrument. Students were assured responses were anonymous. Results were analyzed with Winsteps 3.63.2, a Rasch measurement software tool developed by John Linacre. Further details on this tool are presented below. The reliability of this initial test was 0.47 suggesting adjustments to the instrument were necessary before testing it with a heterogeneous population. The instrument was then revised before further testing.

Instrument Testing

The revised instrument was given online to 296 undergraduate business students. Students represent an appropriate sample to test the USP instrument for three reasons: (1) They actively use the Internet; (2) They have security tools provided to them as part of their student fees but are not required to use them; and (3) They are warned about security issues, but there is no control over their actual security practices exercised by the university, just like for typical home users. For example, the password requirements at the institution the students attend are not as strict as the password requirements measured in this study since they are allowed to make decisions about how often they change their passwords, and how strong they make their passwords. Further, while students

[2] Some experts recommended never writing passwords down, while others recommended that individuals would be better served by creating the most complex passwords they can and write them down, but store them in a secure location.

are told about the importance of using anti-virus software, the usage of this software is not mandated.

The Rasch Rating Scale Model (RSM) (Wright and Masters 1982) was used to test the instrument in a similar manner to previous information systems research (Dekleva and Drehmer 1997). Details of RSM are provided in Appendix A. Relying on RSM instead of classical test theory is appropriate in this study as RSM allows for items in one scale to have multiple response formats, it determines how well questions measure a latent trait, studies the responses by individual as well as the population, and statistically tests the assumption that thresholds between categories are consistent (Hambleton et al. 1991; Hays et al. 2000). Ultimately this provides much greater support for whether or not the responses being collected from individuals are truly what the individuals intended. We applied several analytical procedures to assess the quality of the instrument including dimensionality, reliability, fit, rating scale analysis, and validity evidence. The different tests are described in Table 2.

Dimensionality[3]

We examined the dimensionality of the data set via principal component analysis of the residuals from the RSM. Items were condensed to reflect the construct of interest that was measured reducing the number of items from 51 to 45. For instance, certain yes/no questions such as the presence of a wireless network in the home were removed from analysis, and only respondents that used home wireless networks were analyzed on this trait. Items were grouped based on similarity of scales, with two scales being present, with one being a 5-point scale (0 to 4) and the other a dichotomous scale. An initial analysis of the data showed that there was not a unimodal distribution of the items on the 5-point scale so the scales were re-analyzed on a 3-point scale (security practices were regularly performed, sometimes performed, or never performed). The resulting 3-point scale did display a unimodal distribution and was used for the subsequent analyses.

The dimensionality of the data set was analyzed by extracting its variance using the software WINSTEPS version 3.63.2 and converting it to transformed Eigenvalues, which represent how much of the unexplained variance is explained by each dimension. This test indicated that there might be one dimension beyond the Rasch model explaining enough variance to be of substantive interest. We therefore conducted a parallel analysis, which calculates a more precise Eigenvalue. This analysis bootstraps a dataset that perfectly fits the model and then compares the Eigenvalues to those calculated from the original dataset (Wolfe 2008). Because the original transformed Eigenvalue is more than the bootstrapped value for the USP instrument, but not for residuals, it is determined that the data exhibit unidimensionality.

The component loadings were then analyzed. Items with more than nine percent of their variance explained by the bi-serial point measure correlation were considered to load together as part of the Rasch model. The bi-serial correlation represents the correlation between the item score and the total score, with the difficulty of the items taken into consideration. Item scores that do not correlate with the total score above the 9% cut off need to be dropped from further analysis (Pett 1997). Based on this analysis, 14 items were dropped due to not being part of the Rasch model. Five items related to the writing and storing of passwords. This seems appropriate since there was disagreement between experts in developing these items on whether or not this was a good or a bad thing to do. Information security professionals also seem to disagree on this practice (Kotadia 2005; Ranalli 2003). One item from access to computers by others, three from wireless network settings, one item from firewall usage, one item from popup blocking software, and one item from following links from within email were dropped. In each case, there were multiple items measuring similar concepts. In these instances, the other items measuring the behaviors have simply captured more variance and are reflected in the Rasch model. The restriction of access to computers item was dropped, and we believe this concept was captured by access to computers by others and the screen saver items, which are accomplishing similar tasks. Finally, the using caution when opening attachments item was dropped, and we believe that this concept is captured by the usage of anti-virus software. Therefore, the 31 items that remain were used for further analyses.

Reliability

We examined reliability to determine how dependable and repeatable the test scores are. This reliability factor calculates the ratio of true item variance to observed item variance and shows how consistent measurements are for individuals or groups of a population (Osterlind 2006). The reliability of the 31-item instrument shows an acceptable reliability of 0.72.

[3] Tables supporting the information in this section, including item loading with bi-serial correlation and variance explained, item quality tests, and rating scale analyses are available from the first author.

Table 2. Validation Tests Performed

Validation Test	Purpose
Dimensionality	Determines whether the appropriate Likert scale is being used and whether respondents are answering survey questions consistently with how the researcher intends.
Reliability	Determines how dependable and repeatable the survey responses are.
Item Loading	Determines whether items intended to measure a portion of a latent construct indeed do so.
Item Quality Testing	Determines how well model predicts the responses of the individuals. This includes testing for (item fit), and (person fit).
Rating Scale Analysis	A series of eight tests used to determine whether the instrument works as designed.

Item Quality

One advantage of using RSM is the ability to determine how appropriate the model is for the data. This includes testing the assumptions of the model, determining the accuracy of the model's predictions, assessing the overall fit of the model to the data, and assessing the fit of the individual components of the measurement context to the model (Wolfe 2007). Model assumptions were analyzed as part of the dimensionality analysis. Item fit and person fit measures were also analyzed to determine whether or not participants responded to items as predicted (Hambleton and Swaminathan 1985). All analyses show acceptable level of fit, confirming the structural validity of the USP instrument.

Rating Scale Analysis

The rating scale analysis is used to determine whether the instrument works as intended. When an instrument is administered, a certain set of responses are available for the respondent. Performing this analysis determined that the respondents answered using the intended scale and the available responses captured the USP scale as intended.

Testing the USP Instrument

While the development of the USP instrument followed a set of rigorous procedures, the instrument is not considered valid until a test of the instrument is performed using its finalized form. For this final test, we collected data using online and paper-based versions of the survey. The paper survey was administered to attendees of a soccer tournament. The online survey was first sent to a convenience sample of professionals the researchers had contacts for, asking them to also forward the request. Additional data was collected through a request to participate sent to subscribers of a graduate student listserv. Finally, a number of small businesses disseminated a request to have their employees complete the survey. These small businesses included local accounting firms, a software development company, and an Internet development company. A total of 324 surveys were received, 55 on paper and 269 online. One survey from a participant who was under the age of 18 was eliminated along with 44 incomplete surveys. Hence, 279 surveys were used for data analysis: 52 paper responses and 227 online responses. 142 responses came from the graduate listserv, 63 responses from the email forward, 52 responses from the soccer tournament, and 22 from small business employees. Over half of the respondents are female (55.3%). The majority are Caucasian (85.6%). The income is well distributed between four categories of income, with no group containing more than 35% and no group containing less than 20%. The average age of respondents was 35.3 with a minimum of 20 and a maximum of 83. Subjects have been using computers an average of 16.7 years with a range of two to 53 years. A rating scale analysis performed on the collected data revealed that all eight of Linacre's (2002) suggested criteria were met. These results confirm that the USP scale is appropriate to use with a heterogeneous population. An annotated version of this final USP instrument is presented in Appendix B.

When hypothesizing theoretical models, not only is it important to test the hypotheses in the model, but it is also important to define and test the nature of the constructs in the model. Research models can be composed of any combination of reflective, formative, and multi-dimensional constructs (Petter et al. 2007). The constructs necessary in this research model consisted of three second order constructs (perceived vulnerability, perceived severity, and response efficacy), and two first-order reflective constructs (USP, response cost, and security self-efficacy). The second-order constructs were made up of three first order reflective constructs that each captured a particular threat. Since the dependent variable is a combined measure of individual security behaviors, it was necessary to capture more than one threat so that each behavior measured corresponded to protection from a given threat. Three threats were identified through the interview with experts during the instrument development stage and included file loss, identity theft, and slowing down of the computer's performance. Combined, these three threats resulted in a corresponding threat for each behavior measured.

Table 3. Instrument Adaptation

Dimension	Sources
Perceived Severity	Witte (1996)
Perceived Vulnerability	Witte (1996)
Response Efficacy	Witte (1996)
Response Cost	Neurwirth et al. (Neuwirth et al. 2000), Sheeran and Orbell (Sheeran and Orbell 1996)
Self-Efficacy	Compeau and Higgins (Compeau and Higgins 1995b), Marakas et al. (Marakas et al. 2007), Witte (1996)
USP	Newly Developed

Non-USP Scale Items

The remaining items utilized in this study were adapted from previous literature as validated measures do exist for all the independent variables. PMT researchers developed a scale called the Risk Behavior Diagnosis (RBD) scale, which encompasses severity of threat, susceptibility to threat, self-efficacy, and response efficacy (Witte 1996). Regarding self-efficacy, it was important in this study to follow the recommendation by Marakas and colleagues to adapt the self-efficacy measure to fit the context being studied. PMT researchers also regularly measures response cost (Neuwirth et al. 2000; Sheeran and Orbell 1996) and IS researchers have used similar measures for adapting PMT to the IS domain. These measures are presented in Table 3, along with their source.

Measurement Model

Testing of the measurement model ensures that the measures are valid and properly reflect the theoretical constructs. The reliability, or the internal consistency, of the model was tested along with the convergent and discriminant validity of the measurement items. Reliability was assessed using Cronbach's Alpha and Composite Reliability. All measures displayed satisfactory reliability above the 0.70 threshold (Nunnally 1978), as illustrated in Table 4.

Convergent and discriminant validity were assessed by examining whether items intended to measure one construct were more highly correlated with themselves or with other constructs. Items that loaded the most strongly on their own constructs were considered to have convergent validity. Convergent validity was additionally tested by calculating the Average Variance Extracted (AVE) for each construct, which is the amount of variance that a latent variable component captures from its indicators in relation to the amount due to measurement error. The AVE value for all constructs were above the recommended threshold of 0.50 (Fornell and Larcker 1981), indicating good convergent validity of the items in each construct.

Hypotheses Testing and Results

In order to test the proposed research model in Figure 2, we conducted a survey of 81 graduate students not in an information systems or computer-related major. Given that the focus of this research is on home computer security, students were deemed an appropriate sample to test the proposed model. Prior to testing the relationships hypothesized in the model, the data was tested for reliability and validity. The data was analyzed using Partial Least Squares (PLS), which is necessary when testing the second-order constructs, which are formative measures of the first-order reflective constructs, because it allows for the proper identification of relationships in the model. This translates into a proper assessment of both the measurement model as well as the structural model (Petter et al. 2007).

Discriminant validity was tested by assessing whether the AVE from a construct was greater than the variance shared with other constructs in the model (Chin 1998). Satisfactory discriminant validity is indicated, as the AVE is greater than the squared pair-wise correlation of the latent variables. Discriminant validity was additionally assessed using the cross-loading method (Chin 1998). When evaluating the items across rows, the items loaded most strongly on their intended constructs. Therefore, the measurements satisfied the criteria recommended by Chin (1998)[4].

[4] Tables for these analyses are available from the first author.

Table 4. Reflective First Order Constructs

Construct	CA	CR	AVE
Perceived Severity – File Loss	0.910	0.944	0.849
Perceived Severity – ID Theft	0.863	0.918	0.789
Perceived Severity – Slow Down	0.893	0.933	0.824
Perceived Vulnerability – File Loss	0.851	0.910	0.771
Perceived Vulnerability – ID Theft	0.780	0.872	0.694
Perceived Vulnerability – Slow Down	0.836	0.902	0.756
Response Efficacy – File Loss	0.920	0.949	0.862
Response Efficacy – ID Theft	0.887	0.930	0.815
Response Efficacy – Slow Down	0.874	0.922	0.798
Response Cost	0.783	0.873	0.696
Self-Efficacy	0.725	0.822	0.537

CA: Cronbach's Alpha CR: Composite Reliability

Structural Model

Based on the acceptable analysis of the measurement model, testing of the structural model and proposed hypotheses can ensue. The construct of USP results in a single value for each individual observation. The USP value for each respondent was calculated utilizing the individual score for each respondent provided by the Rasch model. This figure is calculated based on the responses an individual gives and the likelihood of differences over the entire population for a given item.

The structural model was tested using SmartPLS (Ringle et al. 2005) to estimate the path coefficients, which calculates the strength of the relationships between independent and dependent variables. R-squared values were also estimated, in order to display the variance explained by the independent variables. The proposed hypotheses were tested using t-statistics for the standardized path coefficients, by specifying the same number of cases as existed in the dataset and bootstrapping 500 re-samples. One-tailed t-tests were used, as the hypotheses were all direction specific. The results show an r-square of 0.299 for USP, suggesting that approximately 30% of the variance in USP can be explained by the factors identified from the PMT-based research model, with perceived severity, response efficacy, and self-efficacy influencing USP as hypothesized, and perceived vulnerability, negatively influencing USP, opposite of how the relationship was hypothesized. Response cost did not have a significant relationship with USP. Figure 4 shows the results of the PLS test.

These results are consistent with those hypothesized, except that in this study a negative relationship was found between perceived vulnerability and the Unified Security Practices. However, as discussed in the development of the hypotheses, these results are not unexpected. Previous literature shows that when researchers controlled for IS expertise and IT-intensiveness in the industry, they found that when testing with non IS-experts and people who worked in non IT-intensive industries, there was not a significant relationship between perceived vulnerability and intention to adopt anti-malware software (Kumar et al. 2008). Also, perceived vulnerability did not significantly influence security attitude (Herath and Rao 2009b) or whether or not people properly secured their home wireless networks (Woon et al. 2005). However, in the current study, it was found that there was a negative relationship with UPS. This suggests that as perceived vulnerability increases, people will be less likely to perform security tasks and that as perceived vulnerability decreases people will be more likely to perform these tasks. What may actually be happening is a result of measuring actual behaviors instead of behavioral intentions. Once people begin performing a behavior, their intentions no longer matter. Having decided to perform protective behaviors then results in a lowering of the individual's perceived vulnerability. In other words, while at one point in time perceived vulnerability may have been high, when measuring actual behaviors with a variance theory, past vulnerability is not captured. For example, when a person perceives her vulnerability to be high, she has not yet changed her behaviors. Once she has started implementing security tasks to

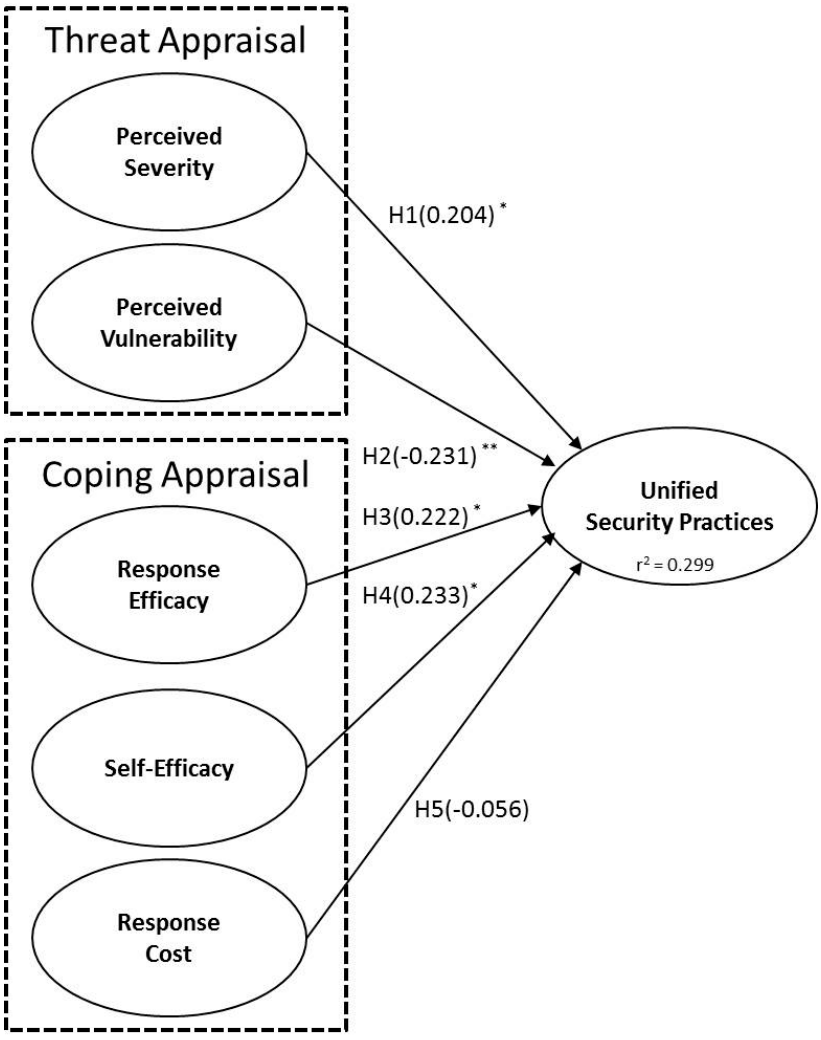

Figure 4. Research Model Results

protect herself from the threat, she may no longer perceive the threat to be high.

Discussion

IS security is a growing concern for researchers and practitioners alike. Since many recognize individuals as one of the weakest links in security, it is important for behavioral security studies to utilize empirically tested theories and provide as much understanding about the security practices of individuals as possible. This study increases researchers' knowledge in both of these areas by testing a previously utilized theory but expanding its explanatory power to include a more encompassing measure of security practices that includes a number of different tasks.

Limitations

Prior to elaborating on the implications of the research, we discuss some limitations. First, the researchers had to make some interpretations based on their analyses of previous research, interviews with experts, and responses of pretest participants. For example, based on conflicts between expert opinions, conflicting literature on this topic, and lack of content validity during technical validation, writing down passwords was not included in the final USP instrument. Using caution when opening links in email also was not included in the USP measure due to results of the analyses. It was concluded that people employ virus scans and spam filtering to prevent this from becoming an issue (if they use properly updated software). Both decisions seemed to be consistent with the advice found in the literature from security scholars, experts, and consumer protection advocates.

However, future studies may discover changes in practices listed in USP due to changes in technology, emerging exploitations of security vulnerabilities and the technological enforcement of information security tool usage. In information security contexts, where technology is always changing, it is important to evaluate the security practices measured and periodically update them to reflect the current state of technology properly. Another limitation of the research is social desirability bias. The survey involved self-reported tasks individuals believe they perform or are saying they perform. It is possible that individuals are saying what they believe they are supposed to say, which does not accurately reflect what they actually do. Future research could overcome this by creating a way to monitor the actual security tasks a person performs. This study also only examined the security practices of respondents from the United States. It could be that data collected from a different country may result in different results due to differences in the cultural norms of the country studied. A cross-cultural study that compares differences between individuals in several countries would provide further insight.

Implications for Researchers and Practitioners

The empirical testing of the PMT-based model with an encompassing measure of unified security practices provides researchers with evidence of the effectiveness at determining the practices of individuals at a more inclusive level. Since this is the approach that is advocated by practitioners, this study addresses core issues that practitioners are advocating. These findings suggest that as a person perceives she is vulnerable to a threat, she will be less likely to do something about it. On the surface, this seems like a disturbing finding, but what it suggests is that as people begin realizing that the threat is severe and that they can do something effective against it, they will be more likely to be doing something about it. This makes sense in a cross-sectional study that examines people's view at one point in time. As an individual is performing a behavior to deal with a threat, he is less likely to be threatened by it, but when he is not being proactive to protect from the threat, the threat is something that stands out in his mind.

The USP instrument results in a continual construct since it measures how individuals perform security practices on a continuous scale. Individually, the items are categorical, but taken as a whole they become continuous. When taking into account the array of practices combined, we can determine whether an individual is performing better than another on a scale from not performing any security tasks at all to performing all security tasks satisfactorily. For example, a person might do a good job at performing backups and utilizing strong passwords, but not at securing their home network. Taken together, these behaviors indicate a better overall security practice than someone only performing backups, although still not a completely satisfactory set of security practices. Analyzing the instrument on a continuum provides the basis for measuring overall improvement at protecting information security.

Another factor captured in the instrument relates to those behaviors that could be automatically performed by the computer itself. In particular, USP captures whether a user has automated the process of updating their updates for their operating system. This automation could happen for other tasks such backing up data, utilization of anti-spyware software and pop-up blocking software (Crossler and Belanger 2012). Based on the design of the survey instrument, individuals who automate these tasks would score highly on the frequency of them being performed. Therefore, this instrument is designed to capture the movement of security behaviors from those that are completely volitional to those that must be enabled and are then automated. Automating security tasks, together with better performance of security behaviors, will provide a greater security environment.

Beyond using theoretical frameworks for explaining security practices, research could take a qualitative approach to understand why individuals perform certain practices and not others. Doing so would provide further insights into constructs that should be included in future theoretical discussions. Through the use of a grounded theory approach, further insights could be obtained and lead to a greater understanding of the underlying reasons individuals perform the security tasks that they do. In fact, most of the theories that ground information security research are of a variance type. Yet, the performance of security behaviors by individuals is likely impacted by their experiences over time. This is where the grounded theory approach using qualitative data collection approaches could be helpful in developing a process model of information security behaviors, which would seek to explain how individuals evolve in their security behaviors over time. A qualitative approach is appropriate if there is a high degree of uncertainty around the phenomenon under study (Eisenhardt 1989; Trauth 2001), which is the case for individual information security practices.

Training programs are used to increase individuals' performance of security tasks (Crossler et al. 2006; Deloitte 2007; Richardson 2007; Schultz 2004). The USP instrument could also be used to assess the effectiveness of security training and awareness programs in experimental settings. Some training programs may be effective on certain aspects of

individual protective security tasks while other training programs may be effective on other tasks. For example, setting up a secured wireless network is a onetime process and then the network will remain secure, while using a strong password and changing it regularly requires constant efforts by individuals. Research might show that these two aspects of recommended security practices require different training to improve the individuals' respective security performance.

By adapting the USP instrument to fit other contexts and threats, researchers will be able to determine the areas that individuals are succeeding at and those that need improvement. This would provide the ability to assess the effectiveness of a group of individuals at performing these tasks over time. For example, by administering the resulting instrument on a regular basis, researchers could determine whether improvements have been made after security training programs are offered. They could then use this information to make recommendations for appropriate training for home users to ultimately improve their security practices and protect their home computers and networks.

A further example of how the instrument could be adapted would be to apply this instrument to users in regards to their mobile devices. As access to the Internet becomes ubiquitous and users need to practice proper security practices on devices beyond their personal computer, the steps individuals need to take to secure themselves are not that different. For example, on a smart phone, updating operating systems and applications need to be done on a regular basis as patches are often released to fix security problems (Becher et al. 2011; Jansen and Scarfone 2008). Additionally, backing up data (Jansen and Scarfone 2008), avoiding phishing attacks (Niu et al. 2008), credit card theft (Jansen and Scarfone 2008), password usage (Jansen and Scarfone 2008), anti-virus usage (Becher et al. 2011), and Wi-Fi safe usage (Becher et al. 2011; Jansen and Scarfone 2008) are all practices that should be in place in a mobile environment. This context provides another great avenue for the future use and testing of the USP instrument.

The USP instrument could also be utilized in other theoretical contexts that explore information security. In particular, this instrument could be used to as the dependent variable in a study utilizing organizational control theory, the theory of planned behavior, and rational choice theory. Doing so would provide even more information towards what causes individuals to protect themselves from security threats. Ultimately a unified theory of individual protective behaviors could be tested that draws from the findings of a number of theories all exploring the same dependent variable.

Researchers could also gain further insight into the protective security practices of individuals as theories emerge that explain these behaviors. With a further understanding of why people behave in a certain way, researchers could make recommendations for solutions that address the causes instead of the symptom. For example, if a low threat appraisal causes a person not to perform given security tasks, researchers could recommend solutions that increase risk perceptions. Such an approach would get to the heart of what caused the weak link in the security of the home user's system. Finally, another avenue for future research with the USB instrument would be how the behaviors that comprise the instrument relate to one another.

Conclusion

In this study, we empirically tested a theoretical model using a newly developed and validated instrument to measure unified security practices. The USP instrument was designed with guidance of IS security experts, and possesses good reliability and validity. The robustness of the USP instrument provides the ability to extend the generalizability of existing PMT-based research to a more complete view of information security practices. As security concerns continue to grow, there is an important role IS researchers can play in understanding not only the technological but also the behavioral aspects of information security. The USP instrument provides one avenue to explore the important behavioral aspects of what security practices individuals actually perform.

References

Ahamad, M., Amster, D., Barrett, M., Cross, T., Heron, G., Jackson, D., King, J., Lee, W., Naraine, R., and Ollmann, G. "Emerging Cyber Threats Report for 2009," Georgia Tech Information Security Center.

Al-Ayed, A., Furnell, S. M., Zhao, D., and Dowland, P. S. "An Automated Framework for Managing Security Vulnerabilities," *Information Management & Computer Security* (13:2) 2005, pp. 156-166.

Anderson, C., and Agarwal, R. "Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions," Twenty-Seventh International Conference on Information Systems, Milwaukee, WI, 2006, pp. 1543-1562.

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

Andrich, D. "Controversy and the Rasch Model: A Characteristic of Incompatible Paradigms?," *Medical Care* (42) 2004, pp. 1-16.

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

Bandura, A. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* (84:2), Mar 1977, pp. 191-215.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., and Wolf, C. "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," Security and Privacy (SP), 2011 IEEE Symposium on, 2011, pp. 96-111.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., and Boss, R. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2) 2009, pp. 151-164.

Cannoy, S., Palvia, P. C., and Schilhavy, R. "A Research Framework for Information Systems Security," *Journal of Information Privacy & Security* (2:2) 2006, pp. 3-30.

Carlson, R. D., and Grabowski, B. L. "The Effects of Computer Self-Efficacy on Direction-Following Behavior in Computer Assisted Instruction," *Journal of Computer-Based Instruction* (19:1) 1992, pp. 6-11.

Chin, W. W. "The Partial Least Squares Approach to Structural Equation Modeling," in: *Modern Methods for Business Research,* G.A. Marcoulides (ed.), Lawrence Erlbaum, Mahway, New Jersey, 1998, pp. 295-336.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. "Management of Information Security: Challenges and Research Directions," *Communications of the Association for Information Systems* (20) 2007, pp. 958-971.

Chung, S. H., Schwager, P. H., and Turner, D. E. "An Empirical Study of Students' Computer Self-Efficacy: Differences among Four Academic Disciplines at a Large University," *The Journal of Computer Information Systems* (42:4) 2002, pp. 1-6.

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

Compeau, D., Higgins, C. A., and Huff, S. "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study," *MIS Quarterly* (23:2) 1999, pp. 145-158.

Compeau, D. R., and Higgins, C. A. "Application of Social Cognitive Theory to Training for Computer Skills," *Information Systems Research* (6:2) 1995a, pp. 118-143.

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

Crossler, R. E., and Belanger, F. "The Quest for Complete Security Protection: An Empirical Analysis of an Individual's 360 Degree Protection from File and Data Loss," in: *18th Americas Conference on Information Systems*, Seattle, WA, 2012.

Crossler, R. E., Belanger, F., and Fan, W. "Determinants of Information Security End User Behavior," in: *2006 Annualy Internation Workshop (WISA 2006) of the AIS Special Interest Group on Netowrk and Internet Security (SIG-SEC)*, Milwaukee, WI, 2006.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:1) 2013, pp. 90–101.

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

Damballa. 2011. "Damballa Threat Report - First Half 2011 " Retrieved April 15, 2013, from https://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf.

Dekleva, S., and Drehmer, D. "Measuring Software Engineering Evolution: A Rasch Calibration," *Information Systems Research* (8:1) 1997, pp. 95-104.

Deloitte. 2007. "2007 Global Security Survey: The Shifting Security Paradigm." Retrieved January 16, 2008, from http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf.

Dhillon, G., and Backhouse, J. "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11:2) 2001, pp. 127-153.

Dinev, T., and Hu, Q. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems* (8:7) 2007, pp. 386-408.

Eisenhardt, K. M. "Building Theory from Case Study Research," *Academy of Management Review* (14:4) 1989, pp. 532-550.

Fagan, M. H., Neill, S., and Wooldridge, B. R. "An Empirical Investigation into the Relationship between Computer Self-Efficacy, Anxiety, Experience, Support and Usage," *The Journal of Computer Information Systems* (44:2) 2003, pp. 95-104.

Fenech, T. "Using Perceived Ease of Use and Perceived Usefulness to Predict Acceptance of

the World Wide Web," *Computer Networks and ISDN Systems* (30:1-7) 1998, pp. 629-630.
Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2) 2000, pp. 407-429.
Fornell, C., and Larcker, D. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1) 1981, pp. 39-50.
Furnell, S. M., Bryant, P., and Phippen, A. D. "Assessing the Security Perceptions of Personal Internet Users," *Computers & Security* (26:5) 2007, pp. 410-417.
Furnell, S. M., Jusoh, A., and Katsabas, D. "The Challenges of Understanding and Using Security: A Survey of End-Users," *Computers & Security* (25:1) 2006, pp. 27-35.
Ghorab, K. E. "The Impact of Technology Acceptance Consideration on System Usage, and Adopted Level of Technological Sophistication: An Empirical Investigation," *International Journal of Information Management* (17:4) 1997, pp. 249-259.
Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2) 2011, pp. 203-236.
Hambleton, R. K., and Swaminathan, H. *Item Response Theory: Principles and Applications* Kluwer Nijhoff Publishing, Boston, 1985.
Hambleton, R. K., Swaminathan, H., and Rogers, H. J. *Fundamentals of Item Response Theory* Sage Publications, 1991.
Hanisch, K. A., Hulin, C. L., and Roznowski, M. "The Importance of Individuals' Repertoires of Behaviors: The Scientific Appropriateness of Studying Multiple Behaviors and General Attitudes," *Journal of Organizational Behavior* (19:5) 1998, pp. 463-480.
Hays, R. D., Morales, L. S., and Reise, S. P. "Item Response Theory and Health Outcomes Measurement in the 21st Century," *Med Care* (38:9) 2000, pp. II-29-II-42.
Herath, T., and Rao, H. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2) 2009a, pp. 154-165.
Herath, T., and Rao, H. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2) 2009b, pp. 106-125.
Im, G. P., and Baskerville, R. L. "A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error," *SIGMIS Database* (36:4) 2005, pp. 68-79.
Jansen, W., and Scarfone, K. "Guidelines on Cell Phone and Pda Security," *NIST Special Publication* (800:124) 2008.
Johnson, R. D., and Marakas, G. M. "Research Report: The Role of Behavioral Modeling in Computer Skills Acquisition: Toward Refinementof the Model," *Information Systems Research* (11:4) 2000, pp. 402-417.
Johnston, A. C., and Warkentin, M. "Fear Appeals and Informaiton Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3) 2010, pp. 548-566.
Kim, E. B. "Information Security Awareness Status of Full Time Employees," *The Business Review, Cambridge* (3:2) 2005, pp. 219-227.
Kindsight. 2012. "Kindsight Security Labs Malware Report – Q3 2012." Retrieved April 15, 2013, from http://www.kindsight.net/sites/default/files/Kindsight_Security_Labs-Q312_Malware_Report-final.pdf.
Kotadia, M. "Microsoft Security Guru: Jot Down Your Passwords," in: *CNET News*, 2005.
Kumar, R. M. L., Park, S., and Subramaniam, C. "Understanding the Value of Countermeasure Portfolios in Information Systems Security," *Journal of Management Information Systems* (25:2) 2008, pp. 241-280.
Lam, J. C. Y., and Lee, M. K. O. "Digital Inclusiveness - Longitudinal Study of Internet Adoption by Older Adults," *Journal of Management Information Systems* (22:4) 2006, pp. 177-206.
Lee, W., Fan, W., Miller, M., Stolfo, S. J., and Zadok, E. "Toward Cost-Sensitive Modeling for Intrusion Detection and Response," *Intrusion Detection* (10:1-2) 2002, pp. 5-22.
Lee, Y., Kozar, K. A., and Larsen, K. R. T. "The Technology Acceptance Model: Past, Present, and Future," *Communications of the Association for Information Systems* (12) 2003, pp. 752-780.
Liang, H., and Xue, Y. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1) 2009, pp. 71-90.
Linacre, J. M. "Optimizing Rating Scale Category Effectiveness," *Journal of Applied Measurement* (3) 2002, pp. 85-106.
Maddux, J. E., and Rogers, R. W. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19:5) 1983, pp. 469-479.
Marakas, G. M., Johnson, R. D., and Clay, P. F. "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability over Time," *Journal of the*

Association for Information Systems (8:1) 2007, p Article 2.

Mullins, R. 2010. "The Biggest Cloud on the Planet Is Owned By ... The Crooks." *Network World* Retrieved April 22, 2010, from http://www.networkworld.com/community/node/58829.

Neuwirth, K., Dunwoody, S., and Griffin, R. J. "Protection Motivation and Risk Communication," *Risk Analysis* (20:5) 2000, pp. 721-734.

Niu, Y., Hsu, F., and Chen, H. "Iphish: Phishing Vulnerabilities on Consumer Electronics," USENIX Workshop on Usability, Psychology, and Security, 2008.

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

Osterlind, S. J. *Modern Measurement: Theory, Principles, and Applications of Mental Appraisal* Pearson Prentice Hall, Upper Saddle River, New Jersey, 2006.

PandaLabs. 2012. "PandaLabs Quarterly Report April - June 2012." Retrieved April 15, 2013, from http://press.pandasecurity.com/wp-content/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf.

Pett, M. A. *Nonparametric Statistics in Health Care Research: Statistics for Small Samples and Unusual Distributions* SAGE Publications, Incorporated, 1997.

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

Ranalli, H. T. "Options for Secure Personal Password Management," in: *SANS Institute*, 2003.

Reardon, J. L., and Davidson, E. "An Organizational Learning Perspective on the Assimilation of Electronic Medical Records among Small Physician Practices," *European Journal of Information Systems* (16:6) 2007, pp. 681-694.

Ricadela, A. "Looming Online Security Threats in 2008," in: *Business Week*, 2007.

Richardson, R. "2007 CSI Computer Crime and Security Survey," Computer Security Institute.

Ringle, C. M., Wende, S., and Will, A. "SmartPLS," Hamburg, Germany, 2005.

Rogers, R. W. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology: Interdisciplinary and Applied* (91:1) 1975, pp. 93-114.

Rogers, R. W., Prentice-Dunn, S., and Gochman, D. S. "Protection Motivation Theory," in: *Handbook of Health Behavior Research: Personal and Social Determinants*, Plenum Press, 1997, pp. 113-132.

Schultz, E. "Security Training and Awareness - Fitting a Square Peg in a Round Hole," *Computers & Security* (23:1) 2004, pp. 1-2.

Sheeran, P., and Orbell, S. "How Confidently Can We Infer Health Beliefs from Questionnaire Responses?," *Psychology & Health* (11:2) 1996, pp. 273-290.

Siponen, M. T., and Oinas-Kukkonen, H. "A Review of Information Security Issues and Respective Research Contributions," *SIGMIS Database* (38:1) 2007, pp. 60-80.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. "Analysis of End User Security Behaviors," *Computers & Security* (24:2) 2005, pp. 124-133.

Stephens, P. "A Decision Support System for Computer Literacy Training at Universities," *The Journal of Computer Information Systems* (46:2) 2005, pp. 33-44.

Straub, D. W. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2) 1989, pp. 147-169.

Trauth, E. "The Choice of Qualitative Methods in IS Research," in: *Qualitative Research in IS: Issues and Trends,* E. Trauth (ed.), IDA Group Publishing, Hershey, P.A., 2001, pp. 1-19.

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

Witte, K. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communication* (1:4) 1996, pp. 317-342.

Wolfe, E. "Edre 6794 Course Presentation," Virginia Tech, 2007.

Wolfe, E. W. "A Bootstrap Approach to Evaluating Person and Item Fit to the Rasch Model," International Objective Measurement Workshop, New York, NY, 2008.

Woon, I. M. Y., Tan, G. W., and Low, R. T. "A Protection Motivation Theory Approach to Home Wireless Security," Twenty-Sixth International Conference on Information Systems (ICIS), 2005, pp. 367-380.

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

Wright, B. D., and Masters, G. N. *Rating Scale Analysis: Rasch Measurement* MESA Press, Chicago, IL, 1982.

Wu, J.-H., and Wang, S.-C. "What Drives Mobile Commerce? An Empirical Evaluation of the Revised Technology Acceptance Model," *Information & Management* (42:5) 2005, pp. 719-729.

Zviran, M., and Erlich, Z. "Identification and Authentication: Technology and Implementation

Issues," *The Communications of the Association for Information Systems* (17) 2006.
Zviran, M., and Haga, W. J. "Password Security: An Empirical Study," *Journal of Management Information Systems* (15:4) 1999, pp. 161-185.

About the Authors

Robert E. Crossler is an Assistant Professor in the Management and Information Systems department at Mississippi State University. He received his Ph.D. in Information Systems from Virginia Tech. His research focuses on the factors that affect the security and privacy decisions that individuals make. He has several publications in the IS field, including *MIS Quarterly*, *Decision Support Systems*, *Computers & Security*, *Journal of Information Systems*, *Journal of Information Systems Security*, Americas Conference on Information Systems, Hawaii International Conference on System Sciences, and many others. He received the 2013 INFORMS ISS Design Science Award for his work in information privacy.

France Bélanger is R. B. Pamplin Professor and Tom & Daisy Byrd Senior Faculty Fellow at Virginia Tech. She researches digital interactions between individuals, businesses, and governments and the related information security and privacy issues. Her work has been published in leading IS journals. She received the 2008 IEEE Education Society Research Award, 2008 Hoeber Research Excellence Award, and 2013 INFORMS ISS Design Science Award. Her work has been funded by agencies, corporations and research centers, including the National Science Foundation. She was Fulbright Distinguished Chair in 2006 (Portugal) and Erskine Visiting Fellow in 2009 (New Zealand).

Appendix A – Details of the Rasch Model

Rasch measurement was designed by Georg Rasch and is similar to Item Response Theory in its statistical underpinnings, but is able to determine how successful a measurement is, allowing for a determination of how well questions measure a latent trait. Rasch measurement models allow researchers to convert dichotomous and Likert (rating) scale observations into linear measures. The difference in using Rasch models over classical test theory statistics is that the individual person is studied rather than populations, allowing for each person to be treated independent of a particular survey question. The Rasch model is generally used to measure test items that have a right or wrong response, but can be used for any item that measures a quantitative attribute or trait. The RSM is formulated as follows:

$$\pi_{nix} = \frac{\exp\sum_{j=0}^{x}(\theta_n - \delta_i - \tau_j)}{\sum_{k=0}^{m}\exp\sum_{j=0}^{x}(\theta_n - \delta_i - \tau_j)}$$

This formula consists of the probability (πnix) that an instrument participant (n) will respond to an item (i) with a certain category x. In this study, θn stands for a person's ability level, δi symbolizes an item's approvability, and τj symbolizes the threshold between two categories. In a polytomous model, τj represents the difficulty of responding in one scoring category versus the next higher category. The rating scale formulation of the Rasch model assumes that the thresholds between scoring categories are constant across items.

The Rasch model is a model in the sense that it is able to statistically determine what the ideal data should look like based on a set of given responses. This approach allows researchers to modify the way that data is collected to match the ideal calculated by the Rasch model, rather than changing the model to fit the data, in essence forcing researchers to ensure their measurement instrument is truly measuring what it is supposed to (Andrich 2004). One way that this is done is through a statistical analysis of the appropriateness of the scale used. For example, if a measure is initially administered on a 7-item scale, through Rasch modeling it is possible to test whether people respond to the item on a 7-item scale or on a 3-item scale. Using the statistical procedures provided by the Rasch model, it is possible to ensure that survey questions are being administered in the same way that respondents are answering them.

The Rasch model calculates a total score, which determines an individual's standing on a given variable. Using this total score, the difficulty of items can be calculated, as well as a person's ability level, which provides a way to determine how well people perform on the measure and how good of a measure an item is. For example, if a person of low ability answers a difficult question correctly it may indicate that this answer was a guess and not an adequate reflection of the person's ability. The more often this happens, the more likely it is that the item is not an appropriate item for the measure. In addition, if a person is inconsistent with her ability level in her responses, indicating guesses or something abnormal about the individual, she can be excluded from the analysis.

There are more detailed information about Rasch modeling on several websites, e.g., http://www.rasch.org/measess/me-all.pdf, http://www.winsteps.com/, http://en.wikipedia.org/wiki/Rasch_model.

Appendix B - Unified Security Behaviors (USP) – Annotated Items

Automatic Updates Questions

[For individuals that have the Windows operating system]…[Answered Yes to lead question]

- Do you have Windows automatic updates turned on?
- Does Windows automatically check for updates?
- Does Windows automatically install updates?

Computer Account Questions

[For individuals who stated other people have access to their personal computer]…[Answered Yes to lead question]

- Do they have different accounts? [For all]
- Have you disabled guest access to your personal computer?
- Have you created or modified the default administrator password on your personal computer?

[For individual who have a wireless network in their house; and who are responsible for administering the wireless network]…[Answered Yes to lead questions]

- Is your wireless network using Wireless Encryption Protection (is it WEP enabled) or Wi-Fi Protected Access (WPA)?
- Is the network name of your wireless network being broadcast?

Software Update Questions

- How often do you check for software updates that are not automatic? (Regularly, Sometimes, Never)
- How often do you manually check for software updates? (Regularly, Sometimes, Never)
- How often is your personal computer scanned for spyware? (Regularly, Sometimes, Never)
- How often do you scan your personal computer for spyware? (Regularly, Sometimes, Never)
- How often do you backup the entire hard drive on your personal computer? (Regularly, Sometimes, Never)
- How often do you backup the important documents your personal computer? (Regularly, Sometimes, Never)

Backup Questions

[For those who store email on their personal computer using software (e.g. Outlook, Outlook Express, Eudora, Thunderbird, etc.)]…[Answered Yes to lead question]

- How often do you backup the email on your personal computer? (Regularly, Sometimes, Never)

Security Education Questions

[For individuals with others living in their house of age to use personal computers]…[Answered Yes to lead question]

- How frequently do you educate others in your house about proper security behaviors such as using anti-virus software, using firewalls, opening email attachments, etc.? (Regularly, Sometimes, Never)

Screen Saver Questions

[For individuals who have personal computer that actively use a screen saver]…[Answered Yes to lead question]

- Does your personal computer require a password to deactivate the screen saver?
- After how many minutes of inactivity does your screen saver come on?

Browser Security Question

- Do you use software to block pop-ups when browsing the Internet?

Firewall Question

- Do you use a firewall on your computer?

Anti-virus Questions

[For those who say that anti-virus software is installed on their personal computer]…[Answered Yes to lead question]

- How often does the anti-virus software scan your personal computer for viruses? (Regularly, Sometimes, Never)
- How often do you scan your personal computers for viruses? (Regularly, Sometimes, Never)

Password Questions

- Approximately, how many accounts do you have that require passwords (please fill in the blank)?
- Approximately, how many of the accounts that require passwords have different passwords (please fill in the blank)?
- What percentage of those passwords do you change quarterly (0 to 100%)?

Strong Password Questions

- What percentage of your passwords meets the criteria for being “strong”?
- What percentage of your banking passwords meets the criteria for being “strong”?
- What percentage of your email passwords meets the criteria for being “strong”?

Phishing Questions

[For individuals who click sometimes or often on e-mails that contain links to web pages.]…[Answered Yes to lead question]

- When do click on these links (check all that apply)?
  - All e-mail
  - E-mail from friends
  - E-mail from your bank
  - E-mail from banks that are not yours
  - E-mail from stores you do business with online
  - E-mail from stores you have not done business with online
  - Other _____
  - I do not click on Internet links from within email messages

Credit Card Questions

Please check all types of websites in which you store your credit card information (check all that apply):

- Government Websites
- Bank Websites
- Companies You Regularly Do Business With
- Companies You Rarely Do Business With
- Companies that have a history of poor security
- All companies that use a secure connection for web transactions (SSL)
- I never store my credit card information on websites