The Information Security Behavior of Home Users: *Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information*

Marc J. Dupuis
University of Washington
marcjd@uw.edu

Robert E. Crossler
Mississippi State University
rob.crossler@msstate.edu

Barbara Endicott-Popovsky
University of Washington
endicott@uw.edu

Abstract

Research examining the information security behavior of individuals with respect to risk has focused primarily on only a handful of constructs; most of which have their roots in Protection Motivation Theory (PMT). However, there is still a lot we do not know about the behavior of individuals. This study examines the information security behavior of home users in the context of one dependent variable: backing up information.

The purpose of this research is largely exploratory with the goal to aid model development in this area. Therefore, an additional set of constructs in various domains are used to measure an individual's risk tolerance and risk perception beyond those generally used in PMT. Additionally, a construct is included to account for an individual's past experiences as it relates to the dependent variable.

The results indicate that an individual's risk tolerance and risk perception with respect to the ethical, financial, and health domains may be important predictors of how they perceive risk in the information security domain, and specifically the task of backing up data. Furthermore, past experiences related to backing up information may help explain some of an individual's current behavior in keeping data backed up.

Keywords: risk perceptions, risk tolerance, backing up data, past experiences, severity, likelihood

Introduction

Computers provide people with the means to perform a wide range of tasks, from running complex applications to storing photographs. The Internet added an additional dimension; it enabled people to shop for gifts, pay bills, perform research, read the news, and communicate with old friends and new. In addition to all of the benefits computers provide to people, there are inherent risks. These risks exist in many different forms, but perhaps most notably as malware (i.e., *mal*icious soft*ware*).

Malware is a type of software that is inserted into a computer with the purpose of causing harm to it or other computers (Garuba, Liu, & Washington, 2008, p. 628). It includes viruses, worms, botnets, Trojan horses, and spyware, and may exist in some form on 25 percent of all home computers (Creeger, 2010, p. 43). Infected computers can be used as part of a botnet to serve malicious goals (e.g., password sniffing, spam proxy, click-fraud perpetuation) ("Malware Threat Rises Despite Drop in Direct Cost Damages.," 2007, p. 19). A computer can be infected through opening a malicious email attachment, visiting an infected website (i.e., drive-by-download), installing infected software, or through other propagation methods (Narvaez, Endicott-Popovsky, Seifert, Aval, & Frincke, 2010).

At the cybercriminal's whim, he can activate the botnets under his control to perform targeted attacks against organizations, institutions, networks (e.g., Department of Defense), and the Internet itself. Fifteen percent or more of all online computers worldwide are part of these botnets (Young, 2008). Given the number of Internet users (79 percent of all U.S. citizens and over 1.3 billion worldwide), this is particularly troublesome (Anderson & Agarwal, 2010, p. 2; Smith, 2010, p. 10).

In an organizational setting, compliance with security policies is mandatory. Policies do not exist for home users, nor are they required to engage in safe security behavior. Organizations have paid a considerable amount of time, money, and attention to information security with positive outcomes. This includes investment in security education, training, and awareness programs (Crossler & Bélanger, 2009; Deloitte, 2007). However, the same has not been done for home users. They are not a homogeneous group and most do not have any organized means of receiving security education, training, or awareness. Furthermore, little is known about what effective security education, training, and awareness would consist of for the home user. Until more concrete information is known about the characteristics associated with their behavior, it will be difficult and likely futile to spend significant resources on information security education, training, and awareness programs for home users.

A significant body of research exists on understanding the security behavior of individuals in an organizational setting (e.g., D'Arcy, Hovav, & Galletta, 2009; Herath & Rao, 2009; Johnston & Warkentin, 2010; Workman, Bommer, & Straub, 2008), while research examining the home user has only more recently began to garner similar attention (*e.g.*, Anderson & Agarwal, 2010; Aytes & Connolly, 2004; Cazier & Medlin, 2006; Crossler, 2010; Crossler & Bélanger, 2006, 2010; Dhamija, Tygar, & Hearst, 2006; J. S. Downs, Holbrook, & Cranor, 2007; Egelman, Cranor, & Hong, 2008; Egelman et al., 2008; Friedman, Hurley, Howe, Felten, & Nissenbaum, 2002; S. Furnell, 2008; S. M. Furnell, Bryant, & Phippen, 2007; S. M. Furnell, Jusoh, & Katsabas, 2006; Hu & Dinev, 2005; Klasnja et al., 2009; LaRose, Rifon, & Enbody, 2008; LaRose, Rifon, Liu, & Lee, 2005; D. Lee, Larose, & Rifon, 2008; Y. Lee & Kozar, 2005; Liang & Xue, 2010; Mannan & van Oorschot, 2008; Nov & Wattal, 2009, 2009; Rhee, Ryu, & Kim, 2005; Salisbury, Pearson, Pearson, & Miller, 2001; Schechter, Dhamija, Ozment, & Fischer, 2007; Woon, Tan, & Low, 2005; M. Wu, Miller, & Garfinkel, 2006; Y. "Andy" Wu, Sherry Ryan, & John Windsor, 2009; Yan, Blackwell, Anderson, & Grant, 2004; Youn, 2005, 2005). Some studies that have been done have only been descriptive in nature without any theoretical underpinning (*e.g.,* Furnell et al., 2007). These studies are useful in understanding "what", but have less value in understanding "why". Those that have been done and grounded in theory have provided some important insight, but have also had inconsistent results with one another (Anderson & Agarwal, 2010; Crossler, 2010; Crossler & Bélanger, 2010; LaRose et al., 2008; Y. Lee & Kozar, 2005; Liang & Xue, 2010; Woon et al., 2005).

Further research in understanding why home users behave in a certain manner with respect to information security is important, including research that goes beyond what has already been done. As long as home users fail to engage in safe and secure computer behavior, organizations, financial markets, governments, and national security will all be at an increased risk. Given the importance of home users in maintaining the integrity of the Internet as well as their own computer, it is imperative that research continues to be done in this area.

Research examining the information security behavior of home users is in its infancy. Information on the scope of the problem has become quite clear, while the explanations based in theory remain both limited and lacking. The problem addressed in this research is: What factors are associated with the backing up of data by home users?

We argue that in addition to the factors commonly employed in understanding the information security behavior of home users, three additional factors—risk tolerance, risk perceptions, and past experience—also play roles in understanding this behavior.

Propositions and Research Issues

The literature suggests several factors may help explain the security behavior of home users. Many of these factors have been incorporated from other empirically supported theories, namely the Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), and Protection Motivation Theory (PMT) (Ajzen, 1985, 1991; Fishbein & Ajzen, 1975; Rogers, 1975, 1983). This has included threat severity, threat vulnerability, self-efficacy, response efficacy, response costs, and social influences. Another factor from Social Cognitive Theory (SCT), locus of control, has also been shown to be an effective indicator of behavioral intentions (Workman et al., 2008). These have all been included in several studies with some efficacy. However, there are three factors that have been included sparingly, if at all, in research on home users. These three additional factors may provide some additional and important insight on the information security behavior of home users. This study examines the role of an individual's risk tolerance and risk perceptions in various domains and past experiences as it relates to backing up information. The purpose of this research is largely exploratory with the goal to aid model development in this area.

Theoretical Foundations

Threat Severity and Threat Likelihood

Threat severity and threat likelihood have their roots in two different theories that have been used to explain the information security behavior of individuals. General Deterrence Theory (GDT) has examined the information security behavior of individuals in organizational contexts in which compliance with security policies is mandatory. GDT has its roots in criminology and emerged in the 1950s as a tool to understand how deterrents prevent or lessen the likelihood of an undesirable act being committed. The idea of effective deterrence was later espoused in work by Gibbs (1975) and Blumstein, Cohen, and Nagin (1978) . The basic premise of the theory is that disincentives to committing a socially undesirable act affect the likelihood that the act will be committed. Disincentives comprise three subconstructs: 1) the certainty of sanction; 2) the severity of sanction; and 3) the celerity of punishment[1] (Blumstein et al., 1978; Gibbs, 1975). Research examining these constructs has generally found the certainty of sanction to be the most effective factor in controlling behavior (Hollinger & Clark, 1983, p. 399). These studies and others would form the basis of later research on the efficacy of deterrence in general, and deterrence as it relates to IS security in particular.

Straub (1990) examined the effectiveness of IS security deterrence efforts in the context of businesses. Three concepts were identified in his model: 1) deterrents; 2) rival explanations; and 3) computer abuse (Straub Jr, 1990, p. 259). Deterrents consisted of two constructs: 1) deterrent certainty; and 2) deterrent severity (Straub Jr, 1990, p. 261). The model was tested through the deployment of a survey to members of the Data Processing Management Association (DPMA). The constructs for deterrents – certainty and severity – correlated with computer abuse, and accounted for 24.2 percent of the variance in abuse (p. 270).

Another theory has similar constructs, but examines it in the context of the individual protecting one's self from a threat. Protection Motivation Theory (PMT) was developed in 1975 by Rogers as an extension of expectancy-value theory to provide a more complete understanding of the effects of fear appeals on attitude change (Rogers, 1975). A fear appeal is

---

[1] Celerity of punishment is something discussed in Gibbs (1975), but has in general been less used in models than either certainty or severity.

a communication regarding a threat to an individual that provides information regarding one's well-being (Milne, Sheeran, & Orbell, 2000, p. 107). It is used "in persuasive messages to scare people in the hopes that the aroused fear will result in the performance of adaptive behaviors" (Roskos-Ewoldsen & Yu, 2004, p. 49). Rogers's work was based in part on earlier research by Lazarus, Leventhal, and Bandura examining threat appraisal. According to Lazarus (1963), "threat, or at least stress reactions mediated psychologically, depend upon the cognitive appraisal of a stimulus" (p. 210).

In PMT, two independent appraisal processes occur as a result of a fear appeal: threat appraisal and coping appraisal. A fear appeal stems from environmental and intrapersonal information. Rogers (1975, 1983) articulated six components of a fear appeal, three for each of the appraisal processes.[2] Threat appraisal consists of: 1) the severity of the perceived threat, based on prior research showing that the manipulation of fear will affect the perceived severity of the threat; 2) the probability that the threat will be realized, noted in prior research to increase as fear-appeals go from low-fear to high-fear; and 3) rewards, both intrinsic and extrinsic, such as personal satisfaction or fulfillment and social acceptance by peers. Fear arousal is an intervening variable with both perceived threat and threat probability. Threat appraisal is believed to inhibit maladaptive responses (e.g., denial, avoidance) (Norman, Boer, & Seydel, 2005, p. 83). However, both intrinsic (e.g., free software through a "warez" site) and extrinsic rewards (e.g., praise from others in the "warez" community for providing software) increase the probability of a maladaptive response.

The original PMT argued that there would be a multiplicative effect between vulnerability, severity and response efficacy on intention (Rogers, 1975). The reasoning was that if any of these components were zero then an adaptive response would not be chosen. This appears reasonable. If a fear appeal indicates that a severe threat exists, but has no probability of occurring, a countermeasure would not be needed regardless of how confident the individual is that it would be effective. Likewise, if a severe threat exists and has a high probability of occurring, but the individual does not believe the countermeasure will be effective, then employing it would be purposeless. While this interaction seems reasonable, it

[2] Rogers (1975) noted that the severity, probability and response efficacy components were previously articulated by Hovland, Janis, and Kelley (1953) based on their work on expectancy-value theories (Hovland, Janis, & Kelley, 1953; Rogers, 1975, p. 97).

has not been supported empirically. In the revised PMT, it was argued that there would be an additive relationship between severity and vulnerability, as well as response efficacy and self-efficacy (Rogers, 1983). Additionally, it was contended that there would be second-order interaction effects between the two appraisal processes. Again, these interactions have not been supported empirically (Cismaru & Lavack, 2007, p. 260). Some research has supported these propositions, but these findings have been highly inconsistent through a number of studies. Finally, many studies have found interactions (multiplicative or additive) not noted above. This includes self-efficacy and vulnerability, severity and response efficacy, cost and response efficacy, and response efficacy and vulnerability (Cismaru & Lavack, 2007, pp. 254–257). This suggests the interactions that may exist within PMT implementations will depend on the context of the study. For example, sample size, threat topic, baseline self-efficacy, baseline perceived threat, and the population the sample is drawn from may all influence the effects found in any given study.

PMT has been used extensively in IS research. Johnston and Warkentin (2010b) argued that both severity and susceptibility would influence response efficacy and self-efficacy (p. 7). Specifically, the greater the perceived magnitude of a threat (severity and vulnerability), the less likely it is that a user will believe he can perform countermeasures effectively. The effect of both severity and vulnerability on behavioral intent is then determined by how they alter perceptions of both response efficacy and self-efficacy. Support was found for severity, but not vulnerability. Directs effects were not tested.

Liang and Xue (2010) forwarded a model that consists of four constructs that have a direct effect on avoidance motivation (part of problem-focused coping). These include: 1) perceived threat; 2) safeguard effectiveness; 3) safeguard cost; and 4) self-efficacy. Perceived threat is determined by two sub-constructs, perceived severity and perceived susceptibility. They hypothesized an interaction between perceived severity and perceived susceptibility, as well as between perceived threat and safeguard effectiveness. Avoidance motivation is noted to have a direct effect on avoidance behavior (p. 397). The results of their study supported all but one of the hypothesized relationships: the interaction between perceived severity and susceptibility was not statistically significant (p. 403).

Finally, in a study examining home users backing up information, Crossler (2010) included direct effects from both perceived security vulnerability and perceived security severity. Crossler (2010) found negative relationships for both constructs, which he noted may be due to those that regularly back up their information perceiving less vulnerability and severity than those that do not.

In this research, the following hypotheses will be tested as part of our underlying base model:

H1: An individual with a high degree of perceived threat severity is more likely to engage in backing up his/her information.

H2: An individual with a high degree of perceived threat likelihood is more likely to engage in backing up his/her information.

Risk Tolerance and Risk Perceptions

An individual's risk tolerance perceptions are in many respects captured by threat severity and threat probability, components already incorporated into the traditional PMT framework. However, there is little known about an individual's risk tolerance and perceptions in other domains and how this may influence or be related to the tolerance and perception of risk in the information security domain. This has the possibility to enrich research in both the information security domain, as well as other domains that examine risk behavior. Given that risky behavior may often prove to be dangerous or costly, this can lead to research examining not just the nature of risk in certain domains, but what can be done to lessen its negative consequences by preventing the behavior in the first place.

Risk evaluation has been examined in several different contexts in many different disciplines. One research tradition examines risk and the use of heuristics in evaluating risks. For example, the representative heuristic involves an evaluation of how closely related or representative one item is to another (Plous, 1993, p. 109). If the person knows the characteristics of one, he may infer that the same characteristics exist for the other. This may work well most of the time, but can also introduce biases. Similarly, an individual may create a heuristic based on his past experience of opening an attachment that was an actual photo instead of malware (based on what he believes). This would make it more likely for him to hold the same beliefs in the future and to perform the same actions. Personal experience is included in this study as a separate construct, but the possibility of a relationship between constructs measuring risk specifically and past experiences would seem to warrant future exploration.

Another component of risk evaluation is in how different types of risks are evaluated. There is a significant amount of important research examining the differential treatment of losses when compared to gains. Specifically, losses are not viewed the same as gains (Kahneman, Slovic, & Tversky, 1982; Kahneman & Tversky, 1996; Tversky & Kahneman, 1991, 1992). Generally speaking, a loss of the same magnitude as a gain will be viewed as more significant. Thus, when something is presented as a possible loss (i.e., negative outcome from a risk), it will generally be perceived to be more significant than a possible gain (i.e., reward). Part of the difficulty in this evaluation from an information security lens is the abstract vs. concrete nature of negative consequences and tangible benefits, respectively.

For example, if an individual chooses not to open an attachment or follow a link in an email because of the perceived risk involved, he is not given feedback that he made the correct choice and averted disaster of some kind. The possible negative outcome remains entirely abstract. In contrast, he denied himself the opportunity to receive a tangible benefit, such as viewing a picture of his granddaughter. This tradeoff may very well lead to opting for the possibility of a tangible benefit. Perhaps even more worrisome is choosing this option and having the computer infected with malware, but the individual either not knowing the computer is infected or not associating it with his earlier action.

An individual's propensity to engage in risks can be measured different ways. The traditional means of measuring whether an individual is risk seeking, risk neutral, or risk averse generally consisted of a single construct (Kahneman & Tversky, 1979). However, this approach fails to consider that an individual's risk tolerance may be highly context specific. Weber et al. (2002) developed several domain-specific risk attitude scales, consisting of: ethical risk, financial risk (investment and gambling), health/safety risk, recreational risk, and social risk. Further, each domain consisted of two separate scales—one to measure risk tolerance and the other risk perceptions. According to Weber et al. (2002), "For prediction purposes, it is immaterial whether observed behavior is the result of beliefs about the riskiness of the choice situation or of attitudes towards (perceived) risk" (p. 267). They noted that it only becomes important if the goal is to change said behavior. Based on research that indicates an individual's risk tolerance may largely be a component of personality (e.g., Plog, 1974), it is hypothesized that greater risk tolerance and lower risk perceptions in the domains previously mentioned will result in lower perceptions of risk likelihood and severity with respect to backing up information.

> **H3: An individual with high risk tolerance in domain X is more likely to minimize threat severity with respect to losing information.**
> **H4: An individual with high risk tolerance in domain X is more likely to minimize threat likelihood with respect to losing information.**
> **H5: An individual with low perceptions of risk in domain X is more likely to minimize threat severity with respect to losing information.**
> **H6: An individual with low perceptions of risk in domain X is more likely to minimize threat likelihood with respect to losing information.**

Past Experiences

A well-known dictum states, "Past behavior is the best predictor of future behavior." Is this also true for past experiences? As previously discussed, the representative heuristic suggests that past experiences cause an individual to make certain decisions related to future behavior. There is also a significant amount of research indicating that if someone has an undesirable experience then they are less likely to engage in behavior that may result in another such experience (e.g., Sonmez & Graefe, 1998). In a study on exploring the impact past travel experiences have on an individual's willingness to travel to a specific region again, Sonmez and Graefe (1998) found that it did have an effect. According to the authors, "While perceptions of risk and feelings of safety during travel appear to have a stronger influence on the avoidance of regions rather than likelihood of travel to them, past travel experience appears to be a powerful influence on behavioral intentions" (Sonmez & Graefe, 1998, p. 177).

The effect past experiences have on future behavior has been examined in the IS domain in general, and within the information security domain in particular. Lee et al (2008) examined the effect of prior virus infection experiences on an individual's intention to adopt virus protection behavior. The construct was significant at the 0.01 level with a $\beta=0.157$. In a study examining risky computing practices in the context of rational choice theory, Aytes and Connolly (2004) examined past experiences by having the participants indicate if they had ever faced negative consequences for not performing a particular security task, and if so, how recently. However, past experiences were not a significant component of either their study or analysis. Past experiences in life generally consist of two components: 1) frequency of those past experiences, and 2) severity. In this study, we hypothesize that each component of past experiences will have an effect on threat severity and threat likelihood of losing information with similar components (past experiences severity and threat severity) having a stronger effect than dissimilar ones (past experiences frequency and threat severity).

H7: An individual with severe negative past experiences related to losing important information is more likely to maximize threat severity with respect to losing information.

H8: An individual with severe negative past experiences related to losing important information is more likely to maximize threat likelihood with respect to losing information.

H9: An individual with a frequent number of negative past experiences related to losing important information is more likely to maximize threat severity with respect to losing information.

H10: An individual with a frequent number negative past experiences related to losing important information is more likely to maximize threat likelihood with respect to losing information.

Table 1 presents the overarching model tested as part of this research. Six different variants of this model are proposed, one for each of the Risk Tolerance and Risk Perception subscales.

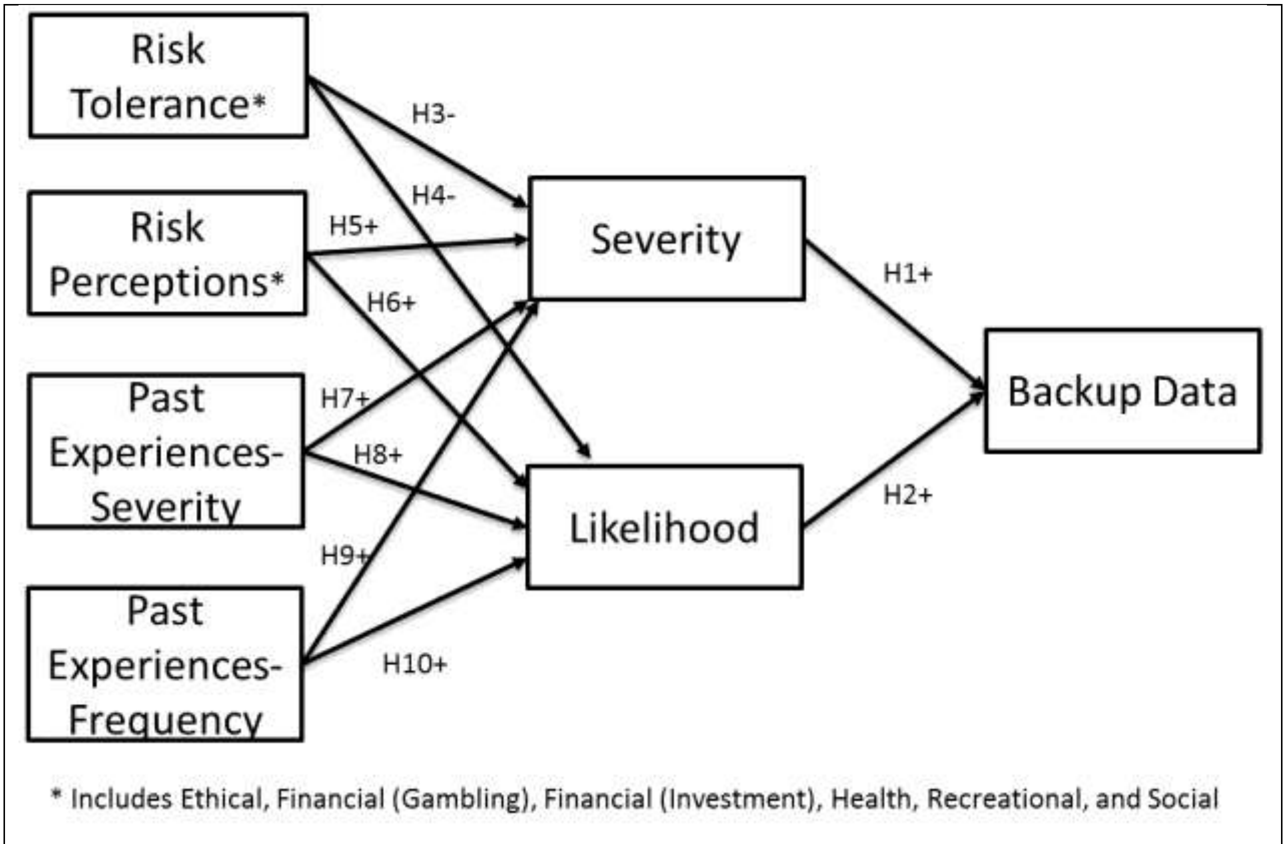

Table 1. Research Model

Intent vs. Behavior

Protection Motivation Theory, Theory of Reasoned Action, and the Theory of Planned Behavior examine an individual's intention to perform a specific behavior. Behavioral intention is presumed to directly impact actual behavior (Maddux & Rogers, 1983; Rogers, 1975). However, the information security domain is constantly changing to the point that intention may not be the best indicator of behavior (Crossler & Bélanger, 2010). Even in an experiment using the prisoner's dilemma, there were significant discrepancies between behavioral intention and actual behavior (Ajzen & Fishbein, 1970). According to the authors, "…a one-to-one relationship is expected if, and only if, BI is very specific to B and measured immediately preceding the performance of B" (Ajzen & Fishbein, 1970, p. 485). Finally, there is precedence in the information security domain to measure behavior, albeit self-reported, rather than behavioral intention (Workman et al., 2008). In the current study, self-reported behavior will be used exclusively. While these measures could have been included in addition to behavioral intention measures, survey length also becomes a concern when measuring complex behavior with various scales (Converse & Presser, 1986; DeVellis, 2003; Rea & Parker, 1997; Tourangeau, Rips, & Rasinski, 2000).

Methods

This study was conducted by recruiting participants using Amazon's Mechanical Turk. The use of Amazon's Mechanical Turk offers several advantages over other recruitment methods (e.g., students, word of mouth, flyers, and electronic postings). For example, turnaround time can be quite quick—all responses in this particular study were collected in less than 24 hours. Furthermore, it is a cost-effective recruitment tool. In this study, participants were credited with 75 cents to their account for their participation. The use of crowdsourcing has increased in popularity and acceptance for these reasons and others (Howe, 2006; Kittur, Chi, & Suh, 2008).

However, it does have some drawbacks. For example, since the users are anonymous, quality control can be quite difficult. Some participants may be "malicious workers" that are simply trying to finish the task to receive payment (Ipeirotis, Provost, & Wang, 2010). While quality of responses is a concern using this method, it is far from unique to this recruitment method. Nonetheless, a quality control question with only one correct answer that was simple and obvious was added to the survey to check for attention, quality, and engagement in the study. The seven participants that failed the quality control question had their data removed from further analysis. Ultimately, different motives and biases may enter the picture due to the use of this method of recruitment; however, it is a common problem for researchers in most recruitment methods employed.

It is not possible to determine the response rate for these participants, but of those that chose to accept the offer and began the survey, 98 percent completed it (N=303). Once the participants that failed the quality control question were removed, we had a remaining sample size of 296. This data suggests a relatively high response rate for this type of methodology given that paper-based mail surveys generally have a response rate of under two percent

(Kotulic & Clark, 2004) with Internet surveys generally even lower (Shih T.-H. & Xitao F., 2008). Although the participants from Amazon's Mechanical Turk are likely more motivated than the general Internet population to complete such surveys. Regardless, the possibility of effects from non-response bias cannot be ruled out. Furthermore, in a study that includes very personal questions for the risk tolerance and perception scales (e.g., "Engaging in unprotected sex"), we believe the web-based format of the survey is the best method to employ in order to minimize social desirability bias.

Finally, the table below compares the age, gender, and geographic distribution for the sample in this study with the U.S. adult population. Although the age of the participants in our study is generally younger than the U.S. adult population, our sample provides a satisfactory range of ages and geographic distributions than what can normally be done through the use of student populations alone. The percentage of participants that identified themselves as white in our study compared to the total number of participants (80.1%) is similar to the U.S. population as well (79.9%).

Table 1: Age, Gender, and Geographic Distribution

	Sample	**U.S. Population**[3]
Age	%	%
18-29	41.55%	22.0%
30-39	25.34%	17.0%
40-49	16.89%	18.2%
50-59	11.49%	18.1%
60+	4.73%	24.7%
Gender	%	%
Male	42.6%	49.1%
Female	57.1%	50.9%
Region	%	%
Northeast	25%	18.01%
Midwest	18.92%	21.77%
South	36.82%	36.91%
West	19.26%	23.31%

[3] Source: U.S. Census Bureau, 2011

Results

The items utilized in this study were adapted from previous literature as validated measures exist for all the variables except for past experience. Umeh (2004) examined past behavior in the context of HIV prevention with the use of a PMT framework. The questions used for the current study are based on the previously validated measures used in Umeh's work with context adapted from other research in IS security (Aytes & Connolly, 2004; D. Lee et al., 2008). However, there are some conceptual differences that make it less than ideal. Given the exploratory nature of this construct, it is considered appropriate to include said measures nonetheless.

The measures for behavior, threat severity, and threat likelihood have been adapted from Crossler (2010) and Witte (1996). With the exception of the risk tolerance and perception scales that employed a 5-point Likert scale measuring degree of likelihood, all other measures have been converted to a 5-point Likert scale consisting of: 1 – Strongly Disagree; 2 – Disagree; 3 – Not Sure; 4 – Agree, and 5 – Strongly Agree. This was done to minimize confusion that can result from frequent changes in scales. These measures are presented in Table 1, along with their source. The exact wording of the measures are presented in Appendix A.

Table 2: Instrument Adaptation

Dimension	Source	Construct Type
Behavior	(Crossler, 2010; Witte et al., 1996)	Reflective
Past Experiences	(Aytes & Connolly, 2004; D. Lee et al., 2008; Umeh, 2004)	Reflective
Risk Tolerance	(Weber et al., 2002)	Reflective
Risk Perception	(Weber et al., 2002)	Reflective
Threat Severity	(Crossler, 2010; Witte et al., 1996)	Reflective
Threat Likelihood	(Crossler, 2010; Witte et al., 1996)	Reflective

Prior to testing the hypotheses in the model, it is necessary to assess the accuracy of the measurement model. This process ensures that the measures are valid and properly reflect the theoretical constructs. The reliability, or the internal consistency, of the model is tested along with the convergent and discriminant validity of the measurement items. Reliability is assessed using Cronbach's Alpha. All of the reflective items except Risk-Perception Health and Social displayed satisfactory reliability above the 0.70 threshold (Churchill, 1979), as illustrated in Table 3. These two Risk Perception measures were removed from further analysis due to the distance they were from the 0.70 threshold.

Table 3. Reliability

Construct	Cronbach's Alpha	AVE
Threat Likelihood	0.829	0.755
Threat Severity	0.945	0.905
Risk Tolerance – Ethical	0.857	0.537
Risk Tolerance – Financial (Gambling)	0.922	0.811
Risk Tolerance – Financial (Investment)	0.806	0.693
Risk Tolerance – Health	0.761	0.578
Risk Tolerance – Recreational	0.834	0.443*
Risk Tolerance – Social	0.777	0.341*
Risk Perception– Ethical	0.814	0.418*
Risk Perception– Financial (Gambling)	0.892	0.748
Risk Perception– Financial (Investment)	0.849	0.660
Risk Perception– Health	0.613*	0.456*
Risk Perception– Recreational	0.849	0.459*
Risk Perception– Social	0.588*	0.235*
Past Experiences – Severity	0.928	0.924
Past Experiences – Frequency	0.882	0.832

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, as illustrated in Table 3, 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 but Risk Tolerance Recreational, Social, and Ethical, as well as Risk Perception Health, Recreational, and Social were above the recommended threshold of 0.50 (Fornell & Larcker, 1981), indicating good convergent validity of the items in each construct. These measures were removed from further analysis.

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). The items loaded higher in their own columns than in the column for other constructs. Furthermore, when evaluating the items across rows, the items loaded most strongly on their intended constructs. Therefore, the measurements satisfy the criteria recommended by Chin (1998).

Structural Model

Based on the acceptable analysis of the measurement model, testing of the structural model and proposed hypotheses can ensue. The structural model was tested using SmartPLS to estimate the path coefficients, which calculates the strength of the relationships between independent and dependent variables. Several separate models were run to test the efficacy of the different independent variables, including separate ones for each domain noted by Weber et al (2002), in providing additional insight into why individuals do or do not back up their data. 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 400 re-samples. One-tailed t-tests were used, as the hypotheses were all direction specific. The results show an r-square of 0.337 for backing up data, suggesting that 33.7% of the variance in backing up data can be explained by the factors identified from the PMT-based research model. The specific hypothesized results are presented in Table 4 and discussed below.

Discussion

The results indicate that using domain specific measures of risk tolerance may help explain an individual's information security risk tolerance and behavior. Specifically, an individual's risk tolerance towards ethical, health, gambling and investment risks warrants further investigation.

Furthermore, similar to how risk tolerance is domain specific, information security behavior may also depend largely on the specific domain. In this study we examined a single type of behavior—backing up information. There are other domains as well. It is unclear the extent to which these new constructs will explain these other information security behavior domains. While an individual's past experiences with data loss appears to help predict current behavior, it is unclear if this will hold true for other types of information security behavior.

The table below summarizes the hypotheses that are supported, those that are not supported, and finally those that are opposite of hypothesized.

Table 4: Hypotheses Outcomes

Hypothesis		Path Coefficient	Supported
H1: An individual with a high degree of perceived threat severity is more likely to engage in backing up his/her information.		0.194	Yes
H2: An individual with a high degree of perceived threat likelihood is more likely to engage in backing up his/her information.		-0.532	Yes+
H3: An individual with high risk tolerance in domain X is more likely to minimize threat severity with respect to losing information.	Ethical	0.133	Yes+
	Financial (Gambling)	0.059	No
	Financial (Investment)	0.011	No
	Health	0.175	Yes+
	Recreational	N/A	N/A
	Social	-0.110	No
H4: An individual with high risk tolerance in domain X is more likely to minimize threat likelihood with respect to losing information.	Ethical	-0.100	No
	Financial (Gambling)	-0.152	Yes
	Financial (Investment)	-0.115	Yes
	Health	0.053	No
	Recreational	N/A	N/A
	Social	N/A	N/A
H5: An individual with low perceptions of risk in domain X is more likely to minimize threat severity with respect to	Ethical	N/A	N/A
	Financial (Gambling)	-0.133	Yes+
	Financial (Investment)	0.094	No
	Health	N/A	N/A

losing information.	Recreational	N/A	N/A
	Social	N/A	N/A
H6: An individual with low perceptions of risk in domain X is more likely to minimize threat likelihood with respect to losing information.	Ethical	N/A	N/A
	Financial (Gambling)	-0.063	No
	Financial (Investment)	-0.124	Yes[+]
	Health	N/A	N/A
	Recreational	N/A	N/A
	Social	N/A	N/A
H7: An individual with severe negative past experiences related to losing important information is more likely to maximize threat severity with respect to losing information.		0.479	Yes
H8: An individual with severe negative past experiences related to losing important information is more likely to maximize threat likelihood with respect to losing information.		-0.208	Yes[+]
H9: An individual with a frequent number of negative past experiences related to losing important information is more likely to maximize threat severity with respect to losing information.		-0.206	Yes[+]
H10: An individual with a frequent number negative past experiences related to losing important information is more likely to maximize threat likelihood with respect to losing information.		0.280	Yes
[+] = Opposite as hypothesized; N/A = Not run due to poor reliability of construct			

Threat severity was supported as hypothesized. With few exceptions (e.g., Crossler, 2010), threat severity has been supported in the hypothesized direction in the literature on a relatively consistent basis. In contrast, threat likelihood (or vulnerability) has proven to be more problematic. In the present study, the relationship between likelihood and backing up data was significant, but in the opposite direction hypothesized. It is unclear why this occurs. One suggestion is that the more an individual backs up her data then the less weight will be given to threat probability (Crossler, 2010).

The role of risk tolerance on performing information security behavior was particularly interesting. Two scales were to have statistical significance on threat severity, but in the opposite direction hypothesized. These were ethical and health risk perceptions. On the other hand two different scales had a significant relationship with the likelihood of losing information. Both of these scales are classified by Weber et al. (2002) as financial risks, gambling and investment. The gambling scale of risk perceptions is negatively related to threat severity, which is significant in the opposite direction hypothesized. The other financial scale, investment, is negatively related to threat likelihood, which is significant in the opposite direction hypothesized. Although, some of these scales were related to threat severity and likelihood in the opposite direction hypothesized they did help to illustrate how one's inherent risk tolerance in one domain may be related to her risk tolerance in the information security domain. As research moves beyond this exploratory study, it will be important to include these scales, especially the financial ones, in understanding why people perform the security behaviors that they do. Including both risk perceptions and tolerance also provides additional insight that one by itself does not.

Understanding the effect that risk perceptions has on threat severity and likelihood has implications for both academics and practitioners. From a researcher's perspective, this provides further insight into what determines a person's perception of threat severity. These findings coupled with other security studies should provide an even better understanding of people's performance at security tasks.

From a practitioner's point of view, these findings allow for better customization of training and awareness programs. As practitioner's can begin classifying the risk perceptions and tolerance of individuals they can better target other perceptions such as threat severity and likelihood to hopefully gain a better change in end-user security behavior. For example, people who are lower risk tolerance to gambling and investment are more likely to believe that a threat of data loss could occur. By understanding this relationship, training programs could be put in place that highlights the likelihood of data loss for participants that have a high tolerance for these factors of risk. Further academic research could experimentally determine the effectiveness of targeted training programs based on these risk tolerances.

Limitations

As with any research, this study is not without limitations. Of primary concern with a survey study of self-report data is social desirability bias. The survey involved individuals responding to questions about security behaviors they believe they perform as well as how they would respond in risky situations. It is possible that individuals are not responding with what they actually do, but rather what they feel they are expected to say. In this study, some constructs had to be excluded due to poor psychometric properties. The lack of these variables could have influenced the effect that other included variables had on the dependent variable. As this study moves forward it will be necessary to revisit the wording on these items to ensure that they can be included in future analyses.

Conclusion

The results from this initial pilot study are quite encouraging. It shows that risk tolerance, risk perception, and past experiences may play a significant role in predicting the information security behavior of individuals.

Future research should further examine risk tolerance and the impact it may have on perceptions of information security risk and costs. There may be additional correlations and interactions worth exploring as well. A larger sample size and the inclusion of other types of information security behavior (e.g., malware prevention) may help provide a greater understanding of the results obtained here, including some of the results that may seem more counter-intuitive.

Although personality may play a significant role in the inherent risk tolerance and perceptions of an individual, the complex nature of risk with its various domains may mean that it simply depends on the context in which risk presents itself. The clearer this becomes to information security researchers then the greater likelihood risky behavior in this domain can be changed for the better.

Bibliography

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Eds.), *Action-control: From cognition to behavior* (pp. 11–39). Heidelberg, Germany: Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. doi:doi: DOI: 10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1970). The prediction of behavior from attitudinal and normative variables. *Journal of Experimental Social Psychology*, *6*(4), 466–487. doi:doi: DOI: 10.1016/0022-1031(70)90057-0

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

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

Blumstein, A., Cohen, J., & Nagin, D. (1978). Introduction. *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*, Report of the Panel on Research on Deterrent and Incapacitative Effects. Washington: National Academy of Sciences.

Cazier, J. A., & Medlin, B. D. (2006). Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times. *Information Systems Security*, *15*(6), 45–55.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295–336). Mahwah, N.J.: Lawrence Erlbaum.

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, *16*(1), 64–73. doi:10.2307/3150876

Cismaru, M., & Lavack, A. M. (2007). Interaction effects and combinatorial rules governing Protection Motivation Theory variables: a new model. *Marketing Theory*, *7*(3), 249–270. doi:10.1177/1470593107080344

Converse, J. M., & Presser, S. (1986). *Survey questions : handcrafting the standardized questionnaire*. Beverly Hills: Sage Publications.

Creeger, M. (2010). CTO Roundtable: Malware Defense. *Commun. ACM*, *53*(4), 43–49. doi:http://doi.acm.org/10.1145/1721654.1721670

Crossler, R. E. (2010). Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. *The 43rd Hawaii International Conference on System Sciences (HICSS)* (p. 10). Koloa, Kauai, Hawaii.

Crossler, R. E., & Bélanger, F. (2006). The effect of computer self-efficacy on security training effectiveness. Proceedings of the 3rd annual conference on Information security curriculum development. doi:http://doi.acm.org/10.1145/1231047.1231075

Crossler, R. E., & Bélanger, F. (2009). The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage. *Journal of Information System Security*, *5*(3), 3–22.

Crossler, R. E., & Bélanger, F. (2010). Determinants of Individual Security Behahaviors (pp. 78–127). Presented at the The Dewald Roode Information Security Workshop, Waltham, Massachusetts.

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

Deloitte. (2007). *2007 Global Security Survey: The Shifting Security Paradigm* (pp. 1–45). Deloitte. Retrieved from http://www.deloitte.com/assets/Dcom-Serbia/Local%20Assets/Documents/rs_Deloitte_Global_Security_Survey_2007.pdf

DeVellis, R. F. (2003). *Scale development : theory and applications*. Thousand Oaks, Calif.: Sage Publications.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. *CHI 2006 Proceedings, Security*. Montréal, Québec, Canada: ACM.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral Response to Phishing Risk. *Proceedings of the Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit* (pp. 37–44). Pittsburgh, PA: ACM.

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems. doi:http://doi.acm.org/10.1145/1357054.1357219

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior : an introduction to theory and research*. Reading, Mass.: Addison-Wesley Pub. Co.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. doi:10.2307/3151312

Friedman, B., Hurley, D., Howe, D. C., Felten, E., & Nissenbaum, H. (2002). Users' conceptions of web security: a comparative study. *CHI '02 extended abstracts on Human factors in computing systems* (pp. 746–747). Minneapolis, Minnesota, USA: ACM.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security*, *2008*(4), 6–9.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*, 410–417.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27–35.

Garuba, M., Liu, C., & Washington, N. (2008). A Comparative Analysis of Anti-Malware Software, Patch Management, and Host-Based Firewalls in Preventing Malware Infections on Client Computers. *Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on* (pp. 628–632). Presented at the Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York: Elsevier.

Herath, T., & Rao, H. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Hollinger, R. C., & Clark, J. P. (1983). Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft. *Social Forces*, *62*(2), 398. doi:10.2307/2578314

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). *Communication and persuasion; psychological studies of opinion change,*. New Haven: Yale University Press.

Howe, J. (2006). The Rise of Crowdsourcing. *Wired*, *14*(6). Retrieved from http://www.wired.com/wired/archive/14.06/crowds.html

Hu, Q., & Dinev, T. (2005). Is Spyware an Internet Nuisance or Public Menace? *Communications of the ACM*, *48*(8), 61–66. doi:Article

Ipeirotis, P. G., Provost, F., & Wang, J. (2010). Quality management on Amazon Mechanical Turk. *Proceedings of the ACM SIGKDD Workshop on Human Computation* (pp. 64–67). Washington DC: ACM.

Johnston, A. C., & Warkentin, M. (2010a). Fear Appeals and Informaiton Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 548–566.

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

Kahneman, D., Slovic, P., & Tversky, A. (1982). *Judgment under Uncertainty: Heuristics and Biases*. Cambridge University Press.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica: Journal of the Econometric Society*, *47*(2), 263–292.

Kahneman, D., & Tversky, A. (1996). On the reality of cognitive illusions. *Psychol Rev*, *103*(3), 582–91; discusion 592–6.

Kittur, A., Chi, E. H., & Suh, B. (2008). Crowdsourcing user studies with Mechanical Turk. *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems* (pp. 453–456). Florence, Italy: ACM.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009). “When I am on Wi-Fi, I am fearless”: privacy concerns & practices in everyday Wi-Fi use. Proceedings of the 27th international conference on Human factors in computing systems. doi:http://doi.acm.org/10.1145/1518701.1519004

Kotulic, A. G., & Clark, J. G. (2004). Why there arent more information security research studies. *Information & Management*, *41*(5).

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting Personal Responsibility for Internet Safety. *Communications of the ACM*, *51*(3), 71–76. doi:Article

LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005). Understanding Online Safety Behavior: A Multivariate Model. *Communication and Technology Division International Communication Association*. New York.

Lazarus, R. S. (1963). A Laboratory Approach to the Dynamics of Psychological Stress. *Administrative Science Quarterly*, *8*(2), 192–213.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445–454. doi:10.1080/01449290600879344

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

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

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Malware Threat Rises Despite Drop in Direct Cost Damages. (2007).*Computer Economics Report*, *29*(7), 12–19. doi:Article

Mannan, M., & van Oorschot, P. C. (2008). Security and usability: the gap in real-world online banking. Proceedings of the 2007 Workshop on New Security Paradigms. doi:http://doi.acm.org/10.1145/1600176.1600178

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1).

Narvaez, J., Endicott-Popovsky, B., Seifert, C., Aval, C., & Frincke, D. A. (2010). Drive-by-Downloads. *The 43rd Hawaii Internal Conference on System Sciences* (p. 10). Koloa, Kauai, Hawaii.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour: Research and Practice with Social Cognition Models* (pp. 81 – 126). Maidenhead: Open University Press. Retrieved from http://purl.utwente.nl/publications/53445

Nov, O., & Wattal, S. (2009). Social computing privacy concerns: antecedents and effects. Proceedings of the 27th international conference on Human factors in computing systems. doi:http://doi.acm.org/10.1145/1518701.1518754

Plog, S. C. (1974). Why Destination Areas Rise and Fall in Popularity. *Cornell Hotel and Restaurant Administration Quarterly Cornell Hotel and Restaurant Administration Quarterly*, *14*(4), 55–58.

Plous, S. (1993). *The psychology of judgment and decision making*. Philadelphia: Temple University Press.

Rea, L. M., & Parker, R. A. (1997). Designing and Conducting Survey Research: A Comprehensive Guide (2nd ed.). *Public productivity & management review.*, *21*(2), 209.

Rhee, H.-S., Ryu, Y., & Kim, C.-T. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. *ICIS 2005 Proceedings*.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, *91*(1), 93.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology : a sourcebook*. New York: Guilford Press.

Roskos-Ewoldsen, D. R., & Yu, H. J. R. (2004). Fear appeal messages affect accessibility of attitudes toward the threat and adaptive behaviors. *GCMM Communication Monographs*, *71*(1), 49–69.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, *101*(4), 165–177. doi:10.1108/02635570110390071

Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007). The Emperor's New Security Indicators, 51–65.

Shih T.-H., & Xitao F. (2008). Comparing response rates from web and mail surveys: A meta-analysis. *Field Methods Field Methods*, *20*(3), 249–271.

Smith, A. (2010). *Home Broadband 2010*. Pew Internet and American Life Project. Washington, D.C.: Pew Research Center. Retrieved from http://pewinternet.org/Reports/2010/Home-Broadband-2010.aspx

Sonmez, S. F., & Graefe, A. R. (1998). Determining Future Travel Behavior from Past Travel Experience and Perceptions of Risk and Safety. *Journal of Travel Research*, *37*(2).

Straub Jr, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255–276.

Tourangeau, R., Rips, L. J., & Rasinski, K. A. (2000). *The psychology of survey response*. Cambridge, U.K.; New York: Cambridge University Press.

Tversky, A., & Kahneman, D. (1991). Loss Aversion in Riskless Choice: A Reference-Dependent Model. *The Quarterly Journal of Economics*, *106*(4), 1039–1061.

Tversky, A., & Kahneman, D. (1992). Advances in Prospect Theory: Cumulative Representation of Uncertainty. *Journal of Risk & Uncertainty*, *5*(4), 297–323. doi:Article

Umeh, K. (2004). Cognitive appraisals, maladaptive coping, and past behaviour in protection motivation. *Psychology & Health*, *19*(6), 719–735. doi:Article

Weber, E. U., Blais, A.-R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making*, *15*(4), 263–290. doi:10.1002/bdm.414

Witte, K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), 317–341.

Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. ICIS 2005 Proceedings.

Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? Proceedings of the SIGCHI conference on Human Factors in computing systems. doi:http://doi.acm.org/10.1145/1124772.1124863

Wu, Y. “Andy,” Sherry Ryan, & John Windsor. (2009). Influence of Social Context and Affect on Individuals’ Implementation of Information Security Safeguards. *ICIS 2009 Proceedings* (p. Paper 70). Presented at the International Conference on Information Systems, AIS Electronic Library.

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: empirical results. *IEEE Security & Privacy Magazine*, *2*(5), 25–31.

Youn, S. (2005). Teenagers’ Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media*, *49*(1), 86–110.

Young, J. B. (2008). Top 10 Threats to Computer Systems Include Professors and Students. *The Chronicle of Higher Education*, *55*(17), A9.

Appendix A

Dependent Variable Measures for Backing up Information

Statement	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
It is likely that I back up all of my important information or files.	1	2	3	4	5
It is possible that I back up all of my important information or files	1	2	3	4	5
I am certain that I back up all of my important information or files	1	2	3	4	5

Independent Variable Measures for the Risk Tolerance (Risk Perception) Scales

Statement	Very Unlikely (Not at all Risky)	Not Likely (Somewhat Risky)	Not Sure (Moderately Risky)	Likely (Very Risky)	Very Likely (Extremely Risky)
Admitting that your tastes are different from those of your friends.	1	2	3	4	5
Going camping in the wilderness, beyond the civilization of a campground.	1	2	3	4	5
Betting a day's income at the horse races.	1	2	3	4	5
Buying an illegal drug for your own use.	1	2	3	4	5
Cheating on an exam.	1	2	3	4	5
Chasing a tornado or hurricane by car to take dramatic photos.	1	2	3	4	5
Investing 10% of your annual income in a moderate growth mutual fund.	1	2	3	4	5
Consuming five or more servings of alcohol in a single evening.	1	2	3	4	5
Cheating by a significant amount on your income tax return.	1	2	3	4	5
Disagreeing with your father on a major issue.	1	2	3	4	5
Betting a day's income at a high stake poker game.	1	2	3	4	5
Having an affair with a married man or woman.	1	2	3	4	5
Forging somebody's signature.	1	2	3	4	5
Passing off somebody else's work as your own.	1	2	3	4	5
Going on a vacation in a third-world country without prearranged travel and hotel accommodations.	1	2	3	4	5
Arguing with a friend about an issue on which he or she has a very different opinion.	1	2	3	4	5
Going down a ski run that is beyond your ability or closed.	1	2	3	4	5
Investing 5% of your annual income in a very speculative stock.	1	2	3	4	5
Approaching your boss to ask for a raise.	1	2	3	4	5
Illegally copying a piece of software.	1	2	3	4	5
Going whitewater rafting during rapid water flows in the spring.	1	2	3	4	5
Betting a day's income on the outcome of a sporting event (e.g. baseball, soccer, or football).	1	2	3	4	5
Telling a friend if his or her significant other has made a pass at you.	1	2	3	4	5

Investing 5% of your annual income in a conservative stock.	1	2	3	4	5
Shoplifting a small item (e.g. a lipstick or a pen).	1	2	3	4	5
Wearing provocative or unconventional clothes on occasion.	1	2	3	4	5
Engaging in unprotected sex.	1	2	3	4	5
Stealing an additional TV cable connection off the one you pay for.	1	2	3	4	5
Not wearing a seatbelt when being a passenger in the front seat.	1	2	3	4	5
Investing 10% of your annual income in government bonds (treasury bills).	1	2	3	4	5
Periodically engaging in a dangerous sport (e.g. mountain climbing or sky diving).	1	2	3	4	5
Not wearing a helmet when riding a motorcycle.	1	2	3	4	5
Gambling a week's income at a casino.	1	2	3	4	5
Taking a job that you enjoy over one that is prestigious but less enjoyable.	1	2	3	4	5
Defending an unpopular issue that you believe in at a social occasion.	1	2	3	4	5
Exposing yourself to the sun without using sunscreen.	1	2	3	4	5
Trying out bungee jumping at least once.	1	2	3	4	5
Piloting your own small plane, if you could.	1	2	3	4	5
Walking home alone at night in a somewhat unsafe area of town.	1	2	3	4	5
Regularly eating high cholesterol foods.	1	2	3	4	5

Independent Variables Measures for Threat Severity & Threat Likelihood

Statement	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
I am at risk for losing important information or files on my computer.	1	2	3	4	5
It is likely that I will lose important information or files on my computer.	1	2	3	4	5
It is possible that I will lose important information or files on my computer.	1	2	3	4	5
I believe that losing information or files on my computer would be a severe problem.	1	2	3	4	5
I believe that losing information or files on my computer would be a serious problem.	1	2	3	4	5
I believe that losing information or files on my computer would be a significant problem.	1	2	3	4	5

Independent Variable Measures for Past Experiences

Statement	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
I have lost important information or files in the past.	1	2	3	4	5
In the past, I have lost a large amount of important information or files.	1	2	3	4	5
I have lost a decent amount of important information or files in the past.	1	2	3	4	5
The information or files I have lost in the past has caused a severe problem.	1	2	3	4	5

In the past, the information or files I have lost has caused a serious problem.	1	2	3	4	5
The information or files I have lost in the past has caused a significant problem.	1	2	3	4	5

Control Question for Attention, Quality, and Engagement

Statement	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
I am able to drive my car to the moon.	1	2	3	4	5