2019

Refining Technology Threat Avoidance Theory

D. Carpenter

Diana K. Young
Trinity University, dyoung1@trinity.edu

P. Barrett

A. J. McLeod

Repository Citation
Carpenter, D., Young, D.K., Barrett, P., & McLeod, A.J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*. doi: 10.17705/1CAIS.04422

Communications of the Association for Information Systems

Volume 44 Article 22

3-2019

Refining Technology Threat Avoidance Theory

Darrell Carpenter
Longwood University, carpenterdr@longwood.edu

Diana K. Young
Trinity University

Paul Barrett
Longwood University

Alexander J. McLeod
Texas State University San Marcos

Recommended Citation
Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining Technology Threat Avoidance Theory. Communications of the Association for Information Systems, 44, pp-pp. https://doi.org/10.17705/1CAIS.04422

Communications of the Association for Information Systems

Research Paper DOI: 10.17705/1CAIS.04422 ISSN: 1529-3181

Refining Technology Threat Avoidance Theory

Darrell Carpenter
College of Business and Economics
Longwood University
carpenterdr@longwood.edu

Diana K. Young
Finance and Decision Science
Trinity University

Paul Barrett
College of Business and Economics
Longwood University

Alexander J. McLeod
Health Information Management
Texas State University San Marcos

Abstract:

Understanding individual threat avoidance motivation and behavior is a critical component in designing effective cyber security solutions for both users and organizations. Technology threat avoidance theory (TTAT) asserts that individuals' perceptions regarding their susceptibility to and the resulting severity of technology threats influence their awareness of the threats, which, in turn, influences their motivation and behavior to avoid them. While TTAT provides cogently and logically explains individuals' technology threat motivations and behaviors, empirical tests have produced equivocal results particularly in terms of the influence of susceptibility and severity on threat perceptions. Due to these inconsistencies in the threat calculus involving susceptibility, severity, and threat, we need more work to improve and understand individual threat motivations. Additionally, TTAT does not account for individual differences such as risk propensity, distrust propensity, and impulsivity that have been shown to affect cyber security behavior. To address these gaps, we present an empirical assessment of a refined TTAT model, which includes individual differences and models the influence of susceptibility on threat perceptions as partially mediated by severity. Results indicate that, while perceived susceptibility is a significant predictor of threat perceptions, severity perceptions partially mediates its effect. Our results also support the inclusion of risk propensity and distrust propensity in the TTAT model as personal characteristics that significantly affect overall threat perceptions.

Keywords: Individual Behaviors, Empirical, Psychological Theory, Survey, Security.

This manuscript underwent peer review. It was received 03/26/2018 and was with the authors for 6 months for 2 revisions. Jackie Rees Ulmer served as Associate Editor.

1 Introduction

Understanding individual threat avoidance motivation and behavior represents a critical component in designing effective cyber security solutions for both users and organizations. In 2009, the United States National Security Agencies' Information Security Director, Richard Schaeffer, stated that, if individuals simply implemented known best practices, regularly monitored network activity, and applied proper configuration policies, both they and their organizations could avoid over 80 percent of cyber incidents (Zetter, 2009). The cyber security landscape today remains remarkably similar. For example, the Online Trust Alliance (OTA) recently reported that 91 percent of the 2016 cyber incidents it analyzed were preventable and noted that most resulted from unpatched software, misconfigured devices, unencrypted data, employee errors, hazardous links, or obsolete technology (Spiezle & Wilbur, 2017). Further, the Open Web Application Security Project recently added "insufficient attack detection and prevention" to its list of the ten most critical security risks (OWASP, 2017) to recognize the pervasive failure of individuals and organizations to implement well-known security measures that detect and prevent many types of attacks (Williams, 2017).

The 2016 Democratic National Committee (DNC) email server incident clearly exemplifies the failure to implement established best security practices (Lipton, Sanger, & Shane, 2016). Despite being a critical component of the United States electoral system, the DNC failed to adequately assess its susceptibility to cyber compromise and failed to implement the most basic detective and preventative security controls. This decision rendered DNC IT staff members unable to identify a suspect device when the FBI notified them that a compromise had occurred. Accordingly, the DNC did not take the FBI warning seriously, and nearly seven months passed before it initiated an incident response. During that time, multiple employees, including John Podesta, the chairman of Hillary Clinton's presidential campaign, received phishing emails and inappropriately clicked on links in those messages that allowed hackers to access the trove of emails that WikiLeaks (2016) later released. Clearly, had DNC leaders conducted a more thorough risk assessment, proactively adopted robust network-monitoring tools, and implemented a more aggressive user-training program, they might have mitigated the impact of the incident.

The fact that preventable cyber incidents continue to occur raises the question of why individuals do not do more to avoid security threats. In an effort to answer this question, Liang and Xue (2009) proposed the technology threat avoidance theory (TTAT), which asserts that individuals' perceptions about their susceptibility to and the resulting severity of technology threats influence their awareness of the threats (known as the threat calculus). This threat calculus, in turn, influences their motivation and behavior toward avoiding them. While TTAT cogently and logically explains individuals' technology threat motivations and behaviors, empirical tests have produced inconsistent results (Arachchilage & Love, 2014; Manzano, 2012; Young, Carpenter, & McLeod, 2016). As for why, one potential explanation might lie in an inaccuracy in the specified relationship between susceptibility and severity as antecedents of the overall threat perception. Liang and Xue (2010) modeled threat susceptibility and threat severity as having both direct and an interactive effect on avoidance motivation. However, in reviewing empirical studies in this domain, we found that the relationships between susceptibility, severity, and threat perceptions appear significant in some studies and insignificant in others (Manzano, 2012; Vance, Anderson, Kirwan, & Earle, 2014).

Further, we argue that TTAT fails to consider important individual differences when assessing avoidance motivation. Prior literature has shown that individuals' propensities relating to risk, impulsivity, and distrust influence their perceptions and decision making processes (Churchill & Jessop, 2010; Hung & Tangpong, 2010). Because research has shown such perceptions and decision-making processes to be central to behavioral motivation in other contexts, we argue that these three personal traits will likely have significant impacts on the model's dependent variables and, thus, that one should consider them as important predictors. We believe that incorporating these individual differences into the TTAT model would allow it to explain technology threat avoidance motivations and behaviors with more nuance. Accordingly, with this research, we examine the following research questions (RQ):

RQ1: Do perceptions about susceptibility influence both perceived severity and perceived threat and, thereby, affect individuals' avoidance motivations and behaviors?

RQ2: Do individual differences such as risk propensity, impulsivity, and distrust propensity influence individuals' technology threat motivations and behaviors?

To answer these questions, we employed a survey research method and structural equation modeling to test a revised TTAT model using a sample of 685 registered Amazon Mechanical Turk workers. Our results

support the revised model in which severity partially mediated susceptibility's influence on threat perceptions. Additionally, we found support for including risk propensity, impulsivity, and distrust in the revised model.

This paper proceeds as follows. In Section 2, we review the existing literature on TTAT, impulsivity, risk propensity, and distrust propensity. In Section 3, we use these prior works to develop our research model and hypotheses. In Section 4, we outline our research method, data collection, and analysis processes. In Section 5, we discuss our results. Finally, in Section 5, we discuss the study's limitations, make suggestions for future research, and conclude the paper.

2 Literature Review

2.1 Technology Threat Avoidance Theory

In the information technology (IT) realm, TTAT (Liang & Xue, 2009) suggests that the way that users perceive a threat influences their motivation to invoke a safeguarding mechanism against it. Liang and Xue (2010) tested their theory verifying the theoretical underpinnings and offering their model to explain technology threat avoidance behavior. The original model includes perceptions of susceptibility, severity, threat, safeguard effectiveness, safeguard costs, self-efficacy, avoidance motivation, and avoidance behavior. A Google Scholar search of previous literature for "technology threat avoidance theory" yielded 88 results (including the two original works). Examining these studies, we found a variety of methods, contexts, and usage. Figure 1 represents the original Liang and Xue (2010) model.

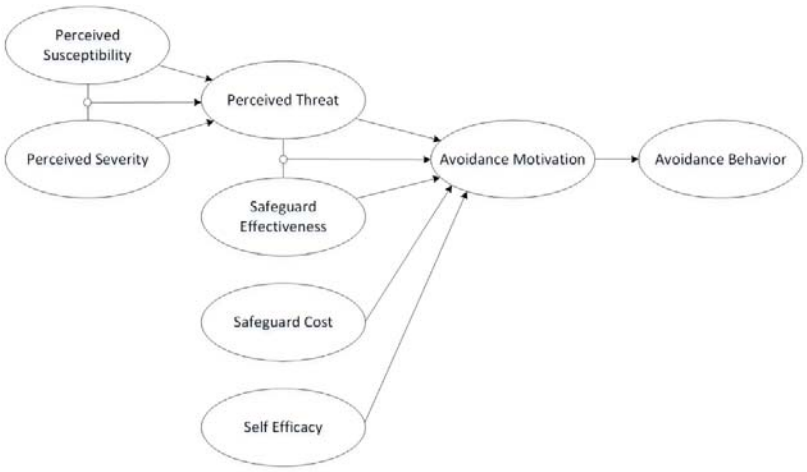

Figure 1. Technology Threat Avoidance Model (Liang & Xue, 2010

Perceived susceptibility refers to an individual's subjective belief that malicious technology will likely affect their devices and systems. Similarly, perceived severity refers to an individual's subjective belief regarding the damage that malicious technology could inflict on their devices and systems. These perceptions both independently and together influence an individual's beliefs regarding a threat's magnitude. That magnitude, along with beliefs regarding the efficacy, costs (time, effort, and money), and ease of implementing a threat safeguard influence one's motivation to avoid the malicious technology, which, in turn, influences one's avoidance behavior.

Analyzing this research stream provided great insight into TTAT and its explanatory value. In originally testing TTAT, Liang and Xue (2010) found that all associations were significant except the interaction between severity and susceptibility. While theory supports these relationships, we found the lack of significance in the interactions surprising and, thus, questioned and reviewed the threat, severity, and susceptibility literature. Several prior studies have tested the full TTAT model, which includes the interaction between susceptibility and severity with differing outcomes (Arachchilage & Love, 2014; Chen & Zahedi, 2016; Manzano, 2012; Young et al., 2016). Manzano (2012) examined the association between susceptibility and threat across two groups: 49 employees at a local beverage company and 32 information technology professionals. They found a significant relationship between susceptibility and threat for local beverage company group but not for the information technology group. Neither the interaction of

susceptibility with severity nor the association of severity with threat was significant depending on which group was under consideration. Arachchilage and Love (2014) found that all associations were significant. Young et al. (2016) found that severity significantly related to threat but that neither susceptibility to threat nor the interaction of severity and susceptibility on threat was significant. Chen and Zahedi (2016) reported the associations of susceptibility and severity significantly related to threat but did not test the interaction of susceptibility and severity. Finally, Bujang and Hussin (2012) suggested a modified full model that did not contain the interaction between susceptibility and severity hypothesized in the Liang and Xu (2009) original TTAT model. However, Bujang and Hussin did not empirically test their newly proposed model.

Recently, Boysen et al. (2017) suggest a change in the threat assessment portion of TTAT in theorizing that susceptibility is an antecedent to severity in the threat calculus (see Figure 2). They tested this theory using the full Liang and Xu (2010) TTAT model. Results indicate significance for all relationships in the threat calculus requiring further examination of this theoretical shift. A brief example may be useful in understanding the argument for a change in current theoretical perspective. Consider Stuxnet, a piece of malware designed specifically to infect a particular type of nuclear centrifuge (Langner, 2011). Computer users concerned about Stuxnet will quickly determine that it only affects certain nuclear centrifuges but that the damage done to those centrifuges can be catastrophic when such systems are infected. Despite its potential for disastrous consequences, typical computer users may not perceive Stuxnet as a severe threat because it is unlikely to affect them. Thus, their perception of low susceptibility directly influences their perception of threat severity. Essentially, a perception of moderate susceptibility becomes a necessary precursor to a perception of severity in the explicit context of threat avoidance motivation and behavior. We do not argue that this phenomenon holds in contexts other than threat avoidance motivation. For example, a subject responding to a survey on Stuxnet may indicate that it is, in general terms, a severe threat. However, that same subject may perceive Stuxnet as a low threat to themselves, a perspective that informs their overall severity assessment and ultimately their threat calculus, and avoidance motivation. To summarize, several researchers have incorporated the full TTAT model in their work to explain the associations between susceptibility, severity, and threat but found mixed results, which indicates that we may need an alternate explanation.

Figure 2. Susceptibility as an Antecedent to Severity (Boysen, McLeod, & Hewitt, 2017)

Some researchers have considered a partial model of TTAT in their research. Rho and Yu (2011) proposed a relationship between susceptibility, severity, and threat and an interaction between susceptibility and severity in a larger theoretically combined model. However, they did not test the proposed model. Mwagwabi, McGill, and Dixon (2014) examined a partial TTAT model and reported significant relationships

between susceptibility and threat and between severity and threat but did not test the interaction between susceptibility and severity. Couraud (2014) invoked a partial model in extending TTAT using risk sensitivity. In this work, severity significantly influenced susceptibility but did not significantly affect self-efficacy. Vance et al. (2014) also tested a partial model. They examined the associations between risk, severity, susceptibility and threat in a "security warning" scenario. They found no significant changes in pretest or post-test for susceptibility but mixed results for severity. Zahedi, Abbas, and Chen (2015) incorporated susceptibility and severity as part of a threat appraisal study but found marginal and mixed results. They did not test the interaction between susceptibility and severity. Browne, Lang, and Golden (2015) used most of the TTAT constructs to create a new security adoption model but did not empirically test their conceptual model. Finally, other empirical and conceptual development studies have used costs and intention constructs when citing TTAT without including susceptibility, severity, and threat. Table 1 overviews TTAT papers that incorporate severity, susceptibility, and threat perceptions.

Table 1. Summary of TTAT Studies that Examine Severity, Susceptibility, or Threat Perceptions

Paper	Notes	Susceptibility	Sus. x Sev.	Severity	Threat
Liang & Xue (2010)	Original TTAT theoretical test.	Sig.	N.s.	Sig.	Sig.
Manzano (2012)	Voluntary working participants comprised experimental group and control group of IT professional participants.	Mixed between groups	N.s.	Mixed between groups	Mixed between groups
Arachchilage & Love (2013)	Changed context to game-based phishing attacks.	Sig.	Sig.	Sig.	Sig.
Young et al. (2016)	Replicates TTAT theoretical test. Broadened context to malware (vs. spyware).	N.s.	N.s.	Sig.	Sig.
Chen & Zahedi (2016)	Examines the online threat avoidance context and focuses on determining which behaviors and perceptions apply to Western vs. Eastern cultures.	Sig.	0	Sig.	Sig.
Mwagwabi (2015)	Extends TTAT to include exposure to hacking as a predictor of perceived vulnerability.	Sig.	0	Sig.	Sig.
Vance et al. (2014)	Uses partial TTAT model examining users' perceptions of risk, severity, susceptibility, and threat.	N.s.	0	N.s.	0
Zahedi et al (2015)	Only uses severity and susceptibility as part of threat appraisal.	Mixed	0	Mixed	0
Xue et al. (2015)	Uses TAM intention and behavior. Not really TTAT.	Sig.	0	0	0

To summarize, TTAT has provided the foundation for many studies, and researchers have used it in various ways. Most researchers have chosen to adopt only pieces of the model; as such, few have tested it completely. Further, research has found mixed results for the relationships between severity, susceptibility, and threat, which indicates that additional work needs to refine and improve the theory. Some researchers have tested additional variables associated with risk, impulsivity, and trust independently. Thus, these variables require further examination using the full TTAT model.

2.2 Impulsivity

Impulsivity is a complicated, multifaceted concept that refers to an individual's propensity to make decisions without thinking about future consequences (Cloninger, Przybeck, & Svrakic, 1991; Eysenck & Eysenck, 1985). Behavioral impulsivity incorporates two distinct factors: impulsive decision making and impulsive activity (Broos et al., 2012; De Wit, 2009; Perry & Carroll, 2008). Numerous studies have begun to examine the neuroscience of inhibition, which they describe as hesitant and limited behavior (Bari & Robbins, 2013;

Dalley, Everitt, & Robbins, 2011), and impulsivity, which they describe as a propensity to make decision without thinking about future consequences (Cloninger et al., 1991; Eysenck & Eysenck, 1985). These works attempt to improve our understanding of the interplay between neurobiology, personality, and situational impacts on impulsive conduct.

Prior research has found associations between emotional studies and impulsivity (Abrantes et al., 2008). For example, individuals who experience a negative or distressful situation may be more likely to make decisions that ignore impulse control (Tice, Bratslavsky, & Baumeister, 2001). As these researchers point out, when upset, people will often indulge impulsive desires in order to make themselves feel better. Emotion regulation is a learned process that research has linked to impulsivity (Schreiber, Grant, & Odlaug, 2012) because it can empower individuals to manage their emotion states to attain beneficial outcomes and, consequently, avoid negative outcomes. Conversely, research has associated the absence of emotion regulation (i.e., emotion dysregulation) with increased impulsivity (Granö, Virtanen, Vahtera, Elovainio, & Kivimäki, 2004).

Impulsivity has the potential to interrupt planning strategies (Churchill & Jessop, 2010; Schweizer, 2002) and, thus, trigger potential risks to individuals, groups, and organizational systems. One can assess it by ascertaining decision making in realistic and speculative situations (Brandstätter, Lengfelder, & Gollwitzer, 2001). Further, broad evidence shows that a relationship exists between impulsive processes, which research refers to as automatic action tendencies and overt avoidance tendencies (Amir, Kuckertz, & Najmi, 2013). These impulsive processes are habits that play an important role in maintaining approach or avoidance behaviors.

In the IS literature, research has shown impulsivity to significantly predict online purchasing habits (Zhang, Prybutok, & Strutton, 2007). Research has theoretically linked it to violations of security practices as a component of general deterrence theory, which regards impulsive actions as a lack of self-control (D'Arcy & Hovav, 2004; D'Arcy, Hovav, & Galletta, 2009; Pahnila, Siponen, & Mahmood, 2007; Siponen, Pahnila, & Mahmood, 2007). Much of the basis for these theorized relationships comes from the criminology literature, which suggests impulsive people focus on the present and often fail to consider the consequences that their actions may have (Nagin & Pogarsky, 2001). Indeed, work in the psychology that has found significant relationships between various forms of impulsivity and narcissism/psychopathy bolsters this characterization (Jones & Paulhus, 2011). Researchers have also modeled impulsivity as a personality trait in security policy compliance decisions and as subject to social control (Cheng, Li, Li, Holm, & Zhai, 2013). However, we know about no empirical study that has examined these theorized links between impulsiveness and security behavior. Understanding the effects of individual impulsivity propensities may elicit insights related to productive and counter-productive threat avoidance behavior in individuals and, thus, play a role in TTAT. In this study, we model impulsivity as an antecedent to avoidance motivation that may influence an individual's decision to take risky actions when faced with a known security threat.

2.2.1 Risk Propensity

Risk propensity refers to an individual's cumulative tendency to engage in or avoid risk (Pablo, 1997; Sitkin & Pablo, 1992; Sitkin & Weingart, 1995) and both persists and evolves with experience (Hung, Tangpong, Li, & Li, 2012). Risk propensity constitutes an important trait to understand when setting policy for decision making (Hung & Tangpong, 2010) and, when left out, can result in policies that present challenges in practice (Bendoly, Donohue, & Schultz, 2006). Decision making related to IT threats, such as general business decisions, has multiple facets, such as combinations of risks in political, financial, operational, and social domains, which feature inherently high ambiguity. Researchers consider risk propensity and ambiguity tolerance to be positively correlated (Lauriola & Levin, 2001) and to have a combined influence on decision making (Hung & Tangpong, 2010). For example, Ghosh (1994) found that ambiguity tolerance had a moderating effect on risk propensity for effectiveness in negotiations.

Risk propensity operates in the decision-making sphere. Researchers generally accept that three main components impact the decision-making process: decision features, individual differences, and situational factors (Einhorn, 1970). The focus on individual differences as an explanatory construct took a step forward in research related to risk aversion in business and finance (Weber, 2001). Studies began to examine risk attitude as an individual difference in a framework of the perceived risk and return in decisions (Weber, Blais, & Betz, 2002). One could certainly argue that risk attitude and risk propensity share similarities and make up part of decision style, and researchers have tested different measures that support that assertion (Mohammed & Schwall, 2009). Overall, individual difference underscores potential effects on judgment and decision making (Appelt, Milch, Handgraaf, & Weber, 2011), and one can assess that effect by determining

actual choices in both realistic and hypothetical scenarios (Levin, Weller, Pederson, & Harshman, 2007). In the same vein, Jackson, Hourany, and Vidmar (1972) created the risk-taking propensity questionnaire, a self-report instrument, to elicit perceptions of risks and benefits to ascertain desirable risk levels in individuals.

Researchers have recognized risk propensity as an important antecedent to security threat perceptions and avoidance behaviors (Moody, Galletta, Walker, & Dunn, 2011; Nguyen & Kim, 2017; Sun & Ahluwalia, 2008; Vance et al., 2014). Nguyen and Kim (2017) studied the level of association between 244 university students' risk propensities and their information-avoidance behaviors. They found significant associations between individuals' risk propensities and their threat perceptions and behaviors. Finally, Vance et al. (2014) used electroencephalography (EEG) technology to better understand how individuals perceived and responded to information security risks. They found that risk propensity could effectively predict whether or not individuals would disregard security warnings both before and after incident exposure. Based on these findings, it appears that risk propensity may play a role in the TTAT model as an antecedent to avoidance motivation.

2.3 Distrust Propensity

An individual's propensity to distrust a technological security solution is rooted in the individual's prior knowledge about unscrupulous behavior or inability to verify the behavior of other actors involved in developing, deploying, and maintaining that security solution (McKnight & Choudhury, 2006). Distrust in this context does not merely refer to the absence of trust but rather to an active state of anticipating malfeasance, incompetence, or insufficient capability by some party involved in creating or maintaining the security solution (McKnight & Chervany, 2001). Distrust propensity refers to one actor's negative perception about another's conduct or potential conduct, while trust refers to one actor's believing that another will not behave opportunistically (Lee, Ahn, & Park, 2015). The actors in a trust relationship generally know one another, while distrust propensity involves both known and unknown actors (Lewicki, McAllister, & Bies, 1998). Distrust propensity forms when an actor has substantial potential to behave opportunistically without detection or explicit means of redress, while actors often build trust relationships on prior experience and structural assurances such as contracts that dictate behavioral standards and means of remediating a failure to perform as expected (McKnight, Kacmar, & Choudhury, 2003).

Researchers have demonstrated distrust towards technology to have negative impacts on user adoption in many contexts. Hsiao (2003) found both value-oriented and reliability-oriented distrust of technology to significantly hinder e-commerce adoption. Sitkin and Roth (1993) modeled value-oriented and reliability-oriented distrust as two facets of distrust that may affect perceptions toward an organization or product. While legal agreements between parties may mitigate reliability-oriented concerns, the availability of legal remedies does not diminish such concerns. This phenomenon has particularly importance in the technology threat avoidance context since many threat mitigation products contain disclaimers that limit any legal remedies that arise from product defects or limitations (Ryan & Heckman, 2003). Similar to Hsiao (2003), Benamati and Serva (2007) found that reliance on technology exacerbated distrust between a technology provider and consumers in online banking. Lin, Shih, and Sher (2007) adopted a slightly different approach by modeling distrust propensity of technology as a component of technology readiness, which they showed to substantially increase the explanatory power of technology adoption models in varying contexts. Thus, the previous literature strongly supports distrust in technology as a barrier to adoption in the general IT context.

In the more specific security technology context, several researchers have discussed distrust propensity due to the potential for abuse of data related to threat deterrent measures. As an example, many organizations use robust authentication mechanisms, such as biometric controls, to protect against unauthorized access and, thus, avoid threats. Prabhakar, Pankanti, and Jain (2003) posited that one might use biometric authentication data to screen for genetic defects among system users without their knowledge or consent. However, using authentication data in this unexpected (but technically feasible) way could have negative impacts on end users and cause them to distrust the biometric technology itself, the system developer, the integrator, or any entity that stores data related to the system. In turn, this distrust could serve as a disincentive for organizations to implement this type of threat-avoidance solution. Other researchers have described methods of using disparate data sources along with security system data to re-identify otherwise anonymous individuals (Salvagnini, Bazzani, Cristani, & Murino, 2013; Schumann & Monari, 2014). In some cases, such as in analyzing keystrokes as a behavioral biometric, collecting the required security system data may lead to privacy risks if exposed (Sun & Upadhyaya, 2015). In this

example, these risks can occur because the information that such an analysis requires also contains sensitive data such as passwords, files accessed, and message data. Recently, public disclosures of governmental meddling related to commercial security products have given rise to additional distrust sentiment among technology consumers. For example, in December, 2013, a Reuters article cited an undisclosed source who claimed that the U.S. National Security Agency (NSA) paid security firm RSA US$10 million dollars to set a known-flawed random number generator as the preferred option in its commercial cryptography products (Menn, 2013) in order to ensure that it could decrypt any traffic encrypted with the faulty cryptographic cipher algorithms. Further, in 2015, Juniper Networks acknowledged that some of their enterprise products contained a cryptographic backdoor that an unknown actor compromised and used an existing "backdoor to create an encryption backdoor" (Smith & Green, 2016). Finally, a recent push from law enforcement agencies across the world to compel commercial companies to provide help in defeating security technologies has exacerbated a climate of distrust among consumers. Law enforcement's aggressive pursuit of cybersecurity backdoors has prompted a group of preeminent cryptographers to engage in the debate concerning law enforcement's access to data secured with various technological solutions (Abelson et al., 2015). While these cybersecurity-centric scholars advocate for strong cryptographic security solutions without backdoors, no one need heed their advice. The potential for collusion between multiple actors, such as governments and product developers, persists, and the consequences of a compromised security solution could be catastrophic. The combination of theoretical misuses of security technology, revelations of flawed products, and governmental efforts to create backdoors in security measures provides a persuasive, if not empirically tested, case for the argument that distrust issues impact threat avoidance behavior.

3 Model and Hypotheses

In this section, we present our refined TTAT research model (see Figure 3) and develop our research hypotheses.

We believe that perceived susceptibility has both a direct and a mediated effect through perceived severity on technology threat perceptions. This rationale rests on the assertion that an individual's awareness of, concern for, or fear of a technology threat will increase when they know they are susceptible to it. Additionally, when individuals know that they are susceptible to a given technology threat, they will become more concerned about the severity of the consequences that result from that threat. Conversely, when individuals know that they are not susceptible to a technology threat, their awareness of, concern for, or fear of that threat and the severity of its consequences will decrease. Based on these arguments, we hypothesize:

H1a: Perceived susceptibility positively influences threat perceptions.

H1b: Perceived severity partially mediates the influence that perceived susceptibility has on threat perceptions.

H1c: Perceived severity positively influences threat perceptions

Beyond our suggested revisions in modeling the influence that perceived susceptibility and perceived severity have on threat perceptions, we adopt and test the remainder of the original TTAT model (Liang & Xue, 2010). Accordingly, based on Liang and Xue (2010) and other studies (Manzano, 2012; Arachchilage & Love, 2014; Chen & Zahedi, 2016; Young et al., 2016) we hypothesize that:

H2: Perceived threat positively influences avoidance motivation.

H3: Safeguard effectiveness perceptions positively influence avoidance motivation.

H4: Safeguard cost perceptions negatively influence avoidance motivation.

H5: Self-efficacy about one's ability to implement a safeguard positively influences avoidance motivation.

H6: Avoidance motivation positively influences avoidance behavior.

Risk propensity refers to an individual's tendency to either avoid or engage in risky endeavors (Pablo, 1997). We believe that individuals with higher risk tendencies will feel less concerned with technology related threats, which will suppress their motivation to avoid those threats. Conversely, we believe that individuals with lower risk tendencies will be more concerned about their susceptibility to technology threats and the potential negative consequences resulting from those threats. Accordingly, we hypothesize that:

H7: Risk propensity negatively influences threat perceptions.

Researchers have defined distrust propensity as negative beliefs regarding another party's conduct (Lee et al., 2015) and demonstrated this distrust to have a negative impact on technology adoption. Since we focus on safeguards for avoiding technology threats in this study, we focus on how distrust impacts threat perceptions. We believe that the more distrusting an individual, the more concern they will have for a technology threat's potential consequences. Accordingly, we hypothesize that:

H8: Distrust propensity positively influences threat perceptions.

Impulsivity refers to individuals' tendency to act with little forethought about the consequences of their actions. We believe that impulsivity suppresses motivation to avoid security threats. For example, when searching for content online, an impulsive individual would be more likely to download the content from a questionable website and lack concern for the fact that the downloaded content may contain a technology threat. The individual's impulsivity to have the desired content causes the individual to not consider the threat's potential consequences. Conversely, a non-impulsive individual would be more likely to thoughtfully weigh the threat's potential consequences and choose to implement a threat safeguard. Accordingly, we hypothesize that:

H9: Impulsivity negatively influences avoidance motivations.

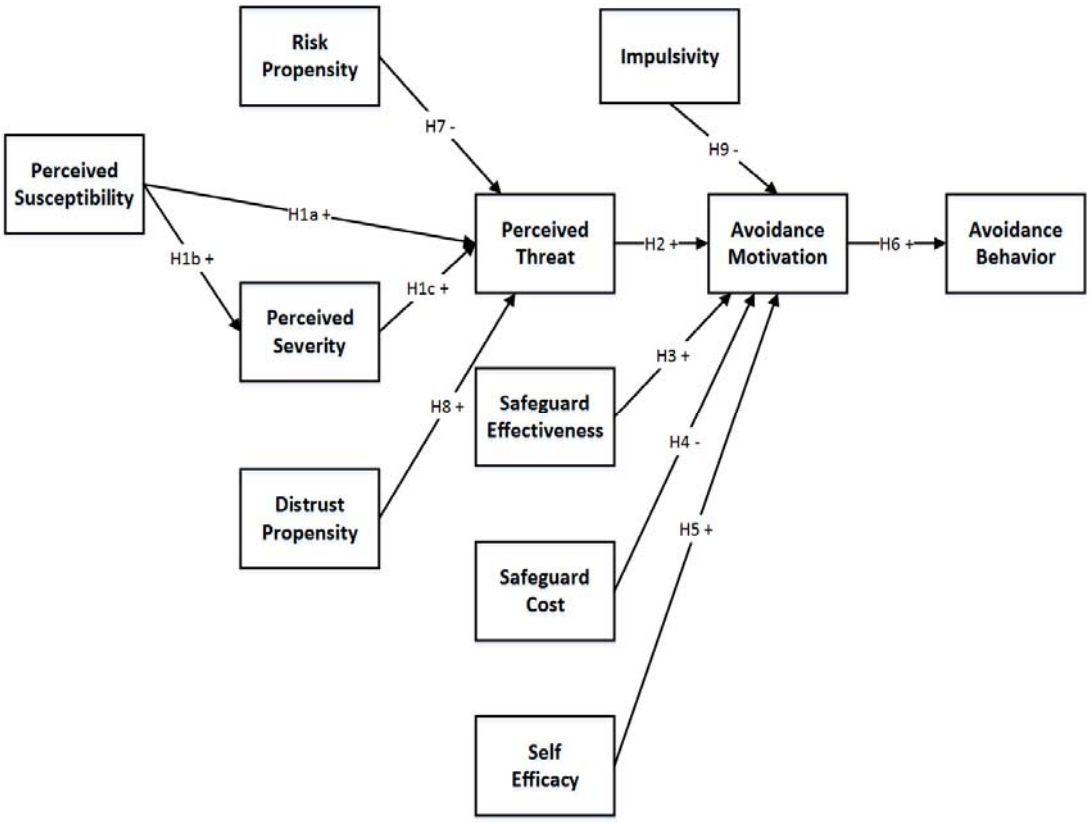

Figure 3. Revised TTAT Research Model

4 Method

We employed a survey research method and structural equation modeling to test our refined research model and hypotheses. We assessed information that 685 registered Amazon Mechanical Turk workers provided. We focused our study on these individuals because most prior TTAT studies have focused on students' technology threat perspectives. Amazon Mechanical Turk workers represent a global community of individuals who rely on their personal computing devices to earn money. Additionally, the community includes individuals who work both full-time and part-time outside of Mechanical Turk, unemployed individuals, and students. As such, we felt the community provided a highly heterogeneous group of

individuals with strong interests in protecting their computing devices from technology threats. The survey instrument included questions regarding respondents' perceptions of their susceptibility to and the severity of the consequences from threats. Below, we outline the measures that we used and the data-collection processes that we employed.

4.1 Measures

We adopted Liang and Xue's (2010) previously validated measures to assess all of the TTAT constructs but modified them based on our review of the literature. First, we modified several items' wording to better fit the malware context. Additionally, we adjusted the perceived severity measure's scale to use a seven-point Likert scale (anchors: 1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 = neutral, 5 = somewhat agree, 6 = agree, and 7 = strongly agree). By making this change, we could assess all constructs using a consistent seven-point Likert scale rather than a survey with mixed semantic differential and Likert items. Finally, we dropped one of the perceived susceptibility items because we felt it focused on future malware susceptibility while all others items focused on current susceptibility. The TTAT section of our instrument comprised four items to measure perceived susceptibility, 10 items to measure perceived severity, five items to measure perceived threat, six items to measure safeguard effectiveness, three items to measure safeguard cost, 10 items to measure self-efficacy, three items to measure avoidance motivation, and two items to measure avoidance behavior. All of the adopted measures exhibited Cronbach alpha coefficients of 0.89 or greater in Liang and Xue's (2010) study.

We also drew measures from the existing literature to assess risk propensity, distrust, and impulsivity. We adopted Nicholson, Soane, Fenton-O'Creevy, and Willman's (2005) six-item measure of risk propensity, which exhibited a Cronbach's alpha coefficient of 0.80 in their study. We used Ashleigh, Higgs, and Dulewicz's (2012) nine-item measure of distrust, which previously exhibited a Cronbach's alpha coefficient of 0.86. Finally, we adopted four items from Grasmick, Tittle, Busik, and Arneklev's (1993) 24-item self-control scale to assess impulsivity. These authors theorized impulsivity to be one of six self-control dimensions. However, factor analysis of the 24 items they used to measure those dimensions resulted in a unidimensional factor structure. While all of the impulsivity items loaded significantly on the unidimensional factor, the authors did not provide reliability metrics for only that portion of the scale.

We included all of the selected measures on an electronic survey instrument that contained seven blocks of items. The first block contained items to assess malware susceptibility and severity perceptions. The second block contained items to assess: 1) malware threat perceptions, 2) beliefs regarding the effectiveness of anti-malware software, and 3) cost perceptions regarding implementation of anti-malware software. The third block contained items to assess self-efficacy beliefs regarding one's ability to effectively install and use the anti-malware software. The fourth block contained items to measure motivation to adopt anti-malware software and actual use of the protective software. The fifth block contained items to measure risk propensity. The sixth block contained items to assess impulsivity and distrust. The seventh block contained various demographic questions. In each block, we randomized the sequence of items to protect against order effects (Shadish, Cook, & Campbell, 2002). Appendix A lists the included items in detail.

4.2 Data Collection

The sample frame of interest included individuals at risk of malware infecting their computing devices. While a great deal of prior TTAT research has focused on students' threat avoidance perceptions and behavior (Liang & Xue, 2010; Young et al., 2016), we felt that we needed to collect the data for this study from a more diverse set of individuals that included both students and adults. Since malware could potentially infect the device of any individual who uses the Internet, we sought data from a broad range of ages, employment status, and geographical locations. Accordingly, we collected data using Amazon Mechanical Turk, a crowdsourcing marketplace.

Amazon (2008) describes Mechanical Turk as a tool that provides task requesters with "access to a diverse, on-demand, scalable workforce and gives workers a selection of thousands of tasks to complete whenever it's convenient". Using the service, task requesters create self-contained human intelligence tasks (HITs) that registered workers can complete to earn monetary rewards. The requester determines the reward size and pays it only if satisfied with the submitted work. Amazon facilitates all financial transactions between task requesters and registered workers.

While Amazon does not release statistics regarding the number of registered Mechanical Turk workers, estimates have suggested that the platform has between 200,000 (Ross, Irani, Six, Zaldivar, & Tomlinson,

2010) and 500,000 individuals (Guarino, 2016) who can complete HITs at any one time. The service has been widely adopted in practice with more than 865,000 active HITs available in January, 2017. Research regarding the service has revealed that Mechanical Turk workers live in a wide variety of locations and represent a broad range of demographic characteristics. Ross et al. (2010) estimated that 57 percent of Mechanical Turk workers live in the United States, 32 percent in India, and three percent in Canada. They estimated that the remaining eight percent of workers live in a diverse set of countries that range from Australia to Nigeria. Further, they found that the average worker age is 31 years old, that 60 percent of workers hold a college degree, that 38 percent work full-time outside of Mechanical Turk, that 31 percent are unemployed, that 33 percent are either a full or part-time student, that 27 percent have annual income below US$10,000, and that 14 percent have an annual income above US$70,000.

Aguinis and Lawal (2012) called Mechanical Turk "an ideal environment to conduct experiments because researchers are able to use real people and real tasks in a controlled environment" (pp. 437). Cheung, Burns, Sinclair and Sliter (2017) subsequently compiled a list of potential validity threats when using Mechanical Turk for research purposes and a set of recommended practices to remediate those threats. Casler, Bickel, and Hackett (2013) compared research responses collected using Mechanical Turk to data collected face to face in a research lab and found no significant differences in the average values of responses.

To collect data for this study, we posted a link to our survey instrument as a HIT on Amazon Turk and offered US$0.50 to the first 650 workers who completed the survey. We chose 650 as a target sample size because a power analysis using G*Power (Faul, Erdfelder, Buchner, & Lang, 2009) indicated that we needed 647 responses to detect small Cohen's f2 effect sizes (Rice & Harris, 2005) using our research model. After cleaning the data and eliminating incomplete surveys, we obtained 644 valid reactions (just shy of the recommended 647 responses).

4.3 Data Analysis and Results

We collected 685 responses to our survey. However, on the day that we posted the HIT, the server that hosted our instrument experienced intermittent connectivity issues. This resulted in several partially complete responses, which we dropped from the sample. Further, following Cheung et al.'s (2017) recommendations, we dropped responses that had indicators of respondent inattentiveness. We used the remaining644 responses for our analysis.

The usable responses came from a highly diverse range of individuals. The youngest respondent was 18, and the oldest was 84. The average age was 34.8 years. Further, 58 percent of our respondents were male, 43 percent were married, 58 percent had children, and 70 percent indicated that they worked full-time. The respondents identified as White/Caucasian (68%) followed by Asian (17%), Black/African American (7%), Hispanic (6%), and other (2%).

The respondents represented a diverse collection of geographical locations. We collected responses from individuals who lived in 38 different countries and six different continents. With that said, most respondents lived in the US (78%) and represented 48 of its 50 states. The second highest number of respondents lived in India (11% of the sample) and the third highest lived in Venezuela (2%). The final nine percent represented 35 different countries. We believe that our sample contained a high number of respondents who lived in the US partly due to our posting our HIT at approximately 10:00 a.m. Central Time the US and Canada. Ross et al. (2010) show that staggering the posting time of HITs results in broader diversity in the geographical location of respondent workers.

We analyzed the collected data using the R language package PLSPM, a partial least squares (PLS) approach for studying complex models based on relationships between sets of latent variables (Chin, 1998). Researchers have shown PLS to: 1) work with both small and large sample sizes, 2) work effectively with both interval and ratio scales, and 3) make minimal demands on residual distributions. The method relies on bootstrap resampling as a non-parametric means of drawing inferences from the provided sample. Accordingly, skewed data does not affect the PLSPM model estimates' precision (Vilares, Almeida, & Coelho, 2010).

4.4 Measure Validation

For analysis purposes, we modeled all items as reflective indicators of the proposed latent constructs. We then followed the two-step structural equation modeling approach that Anderson and Gerbing (1988) recommend by first assessing the measurement model's suitability and then evaluating its veracity.

We also assessed the measurement model's convergent validity, discriminate validity, and construct reliability. To evaluate its convergent validity, we followed the procedure that Gefen, Rigdon, and Straub (2011) outline and examined the "on-factor" loadings. In doing so, we found that four of the distrust indicators did not load significantly on that construct. Consequently, we dropped those indicators from the model and re-ran the analysis without them. Subsequently, we found that all of the remaining indicators loaded strongly on the modeled construct and all but two of the "on-factor" loadings exceeded 0.70 (see Appendix B). The indicators with loadings below 0.70 were for the RSK2 (risk propensity) and SLF1 (self-efficacy), which had loadings levels of 0.65 and 0.60, respectively. As these loadings were just below the recommended threshold of 0.70, we decided to run our model a second time without the two low-loading items included. However, we found no significant differences in beta coefficients, R squared values, reliability coefficients or AVE values between the two models. Since the two items' loadings were just below the recommended threshold and prior research had validated them, we decided to retain the two items in our model and concluded that our measurement model exhibited an acceptable level of convergent validity.

Next, we examined each indicator's cross loadings to assess the measurement model's discriminate validity. We found no "off-factor" loadings within 0.20 of the "on-factor" loadings for all constructs other than avoidance motivation and avoidance behavior. While indicators for those constructs had high cross loadings with each other, we do not believe that it indicates that a problem exists since these constructs have a long and proven record of validity. One must assess indicator loadings with regard to the theorized relationship between the constructs. Both the original TTAT model and our proposed extension assert that avoidance motivation is an antecedent to avoidance behavior. We expected the constructs and their associated indicators to be highly related. To further substantiate the measurement model's discriminant validity, we calculated the square root of the average variance extracted (AVE) for each construct and checked to ensure that it was higher than the construct's correlations with all other constructs as Table 2 shows. We concluded that our model exhibited an acceptable level of the discriminate validity. We assessed construct reliability using Cronbach's coefficient alpha (Wilkinson, 1999). Table 2 includes these coefficients and shows that Cronbach's alpha was above 0.70 for all of the latent constructs, which indicates that, for this particular population of participants, our scales also exhibited an acceptable level of reliability.

Before assessing the structural model's veracity, we employed Harman's (1976) single-factor technique to test for the presence of common method bias. First, we used the fa command in the R pysch package to generate a minimum residual, unrotated factor solution for the 58 indicators in our model. We then inspected the resulting Eigenvalues and scree plot. The unconstrained solution listed eight components with Eigenvalues greater than 1.0 and the Eigenvalue for the ninth component was just under the 1.0 threshold. Cumulatively, those components accounted for 70.56 percent of the variance in the sample. Next, we inspected the scree plot and found two elbows in the graph. The first elbow occurred after the sixth component and the second elbow occurred after the ninth component. Both the Eigenvalues and scree plot indicated that a multifactor solution was appropriate for the collected data. Finally, we re-ran the factor analysis but restricted the output to a single component solution. The single component had an Eigenvalue of 14.39 but accounted for only 22.5 percent of the variance in the sample. Based on these results, we concluded that biases due to common method variance do not present a significant concern for the sample.

Table 1. Construct Descriptive Statistics and Correlations

Name	α	AVE	SEV	SUS	RSK	DIST	THR	EFF	CST	SEF	IMP	MOT	BEH
SEV	0.94	0.66	0.81										
SUS	0.92	0.82	0.36***	0.76									
RSK	0.86	0.59	-0.13***	0.10**	0.76								
DIST	0.89	0.68	0.18***	0.15***	0.19***	0.82							
THR	0.85	0.62	0.68***	0.38***	-0.20***	0.19***	0.79						
EFF	0.93	0.74	0.61***	0.26***	-0.21***	0.10*	0.64***	0.86					
CST	0.87	0.79	-0.38***	0.08+	0.46***	0.11**	-0.27***	-0.41***	0.89				
SEF	0.92	0.58	0.22***	-0.07+	0.01	0.04	0.21***	0.30***	-0.14***	0.76			
IMP	0.84	0.67	-0.21***	0.14**	0.57***	0.34***	-0.18***	-0.19***	0.47***	-0.09*	0.82		
MOT	0.93	0.87	0.42***	0.19***	-0.16***	0.02	0.47***	0.62***	-0.50***	0.22***	-0.19***	0.93	
BEH	0.89	0.90	0.34***	0.15***	-0.08+	0.01	0.36***	0.52***	-0.47***	0.18***	-0.14***	0.82***	0.95

Based on standardized values. Diagonal elements represent the square root of the AVE values
+ p < 0.10, * p < 0.05, ** p < 0.01, *** p < 0.001

5 Results

Finally, to assess the proposed model, we inspected path coefficients and R^2 values of for each construct. Figure 4 shows β coefficients, associated ρ-values, and R^2 values for each dependent variable included in the model. The model accounted for a significant proportion of the variance in perceived severity (R^2 = .14), perceived threat (R^2 = .48), avoidance motivation (R^2 = .48) and avoidance behavior (R^2 = .67).

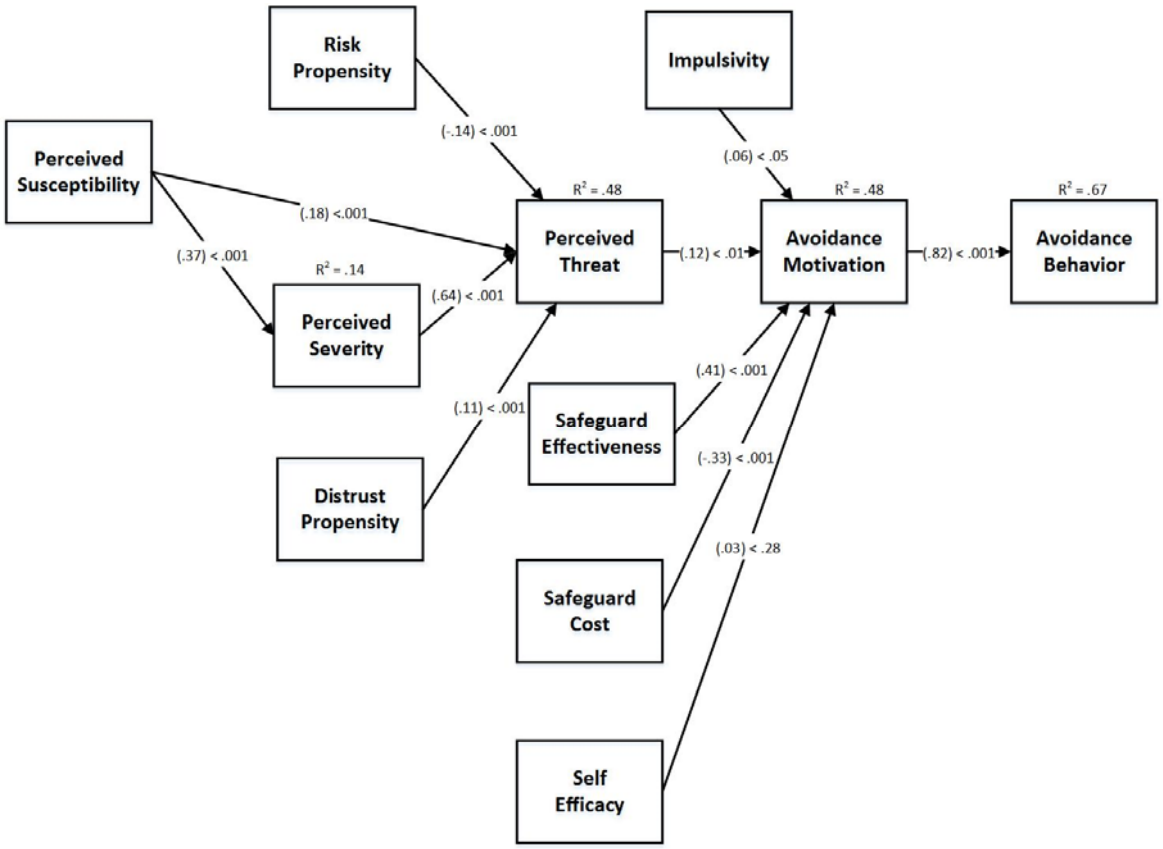

Figure 4. Model Results

On inspecting the model beta coefficient estimates, we found strong support for all but one of our hypothesized relations. Perceived susceptibility had a significant and positive direct effect on perceived severity (β = .37, ρ < 0.001). To assess whether or not perceived severity partially mediated the influence of perceived susceptibility on threat perceptions, we applied Baron and Kenny's (1986) four-step approach to test for the presence of mediation. First, we conducted simple regression tests to confirm that perceived susceptibility was significantly associated with perceived severity (β = .25, ρ < 0.001) and that perceived severity was significantly associated with perceived threat (β = .68, ρ < 0.001). Finally, we conducted multiple regression to confirm that both the direct path from perceived susceptibility to perceived threat (β = .18, ρ < 0.001) and indirect path from perceived susceptibility to perceived threat (β = .37, ρ < 0.001) were both significant.

Accordingly, we found support for our proposal that perceived severity partially mediates the influence of perceived susceptibility on perceived threat. Next, we conducted the Sobel test (Preacher & Leonardelli, 2001) to confirm that the mediation effect was statistically significant (t = 9.33, ρ < 0.002). Accordingly, our results support H1a, H1b and H1c.

We then assessed the beta coefficients and significance values for the other latent constructs in the original TTAT model. Perceived threat was significantly associated with avoidance motivation (β = .12, ρ < 0.01) as were safeguard effectiveness (β = .41, ρ < 0.001) and safeguard cost (β = -.33, ρ < 0.001). However, self-efficacy was not significantly associated with avoidance motivation (β = .03, ρ < 0.28). Accordingly, we found support for H2, H3 and H4 but not for H5. Finally, avoidance motivation was highly associated with avoidance behavior (β = .82, ρ < 0.001), which supports H6.

In terms of the individual differences constructs that we added to the TTAT model, risk propensity was negatively and significantly associated with threat perceptions (β = -.14, ρ < 0.001), which supports H7. Distrust propensity was positively and significantly associated with threat perceptions (β = .10, ρ < 0.001), which supports H8. Finally, impulsivity was significantly associated with avoidance motivation (β = .06, ρ < 0.05); however, the direction of the influence was opposite to what we hypothesized. Thus, we did not find support for H9.

As a final step, we followed the procedures that Cohen (1988) notes to calculate the f2 effect size that each independent variable has on its associated dependent variable. The general guidelines for interpretation of the f2 statistic specify that values greater than or equal to .02 represents a small effect, values greater than or equal to .15 represents a medium effect, and values greater than or equal to .35 represent a large effect. Our analysis indicated that perceived susceptibility had a medium sized effect on perceived severity (f2 = .155) and a small effect on perceived threat (f2 = .054). In addition, perceived severity had a large effect on perceived threat (f 2 = .370), while both risk propensity (f2 = .046) and distrust propensity (f2 = .016) both had a small effect on perceived threat. In terms of avoidance motivation, safeguard effectiveness had a medium effect (f2 = .163), safeguard cost had a small effect (f2 = .118) and threat perceptions had a small effect (f2 = .016). Both self-efficacy (f2 = .002) and impulsivity (f2 = .007) had only a negligible effect on avoidance motivation. Finally, avoidance motivation had a large effect on avoidance behavior (f2 = 2.036).

6 Discussion

Our findings continue to echo Liang and Xue's (2010) original findings and the findings that Young et al. (2016) report in their replication study. For example, perceived susceptibility predicted perceived threat and perceived severity even more vigorously predicted perceived threat. The empirical results supported our decision to examine risk propensity and distrust propensity as potential antecedents to perceived threat. Both constructs were significant and substantially improved the overall R^2 value obtained in the analysis. Respondents with a higher penchant toward risk propensity showed a reduced level of threat perception. In addition, higher distrust propensity predicted increases in perceived threat. These results highlight how individual differences enhance or diminish the perceived severity of threats. Armed with this type of information, organizational leaders could look to identify certain traits among their IT users and initiate training plans to mitigate counterproductive technology threat assessments. We discuss this point in greater detail in Section 6.2.

Contrary to our original hypothesis, we also found that increased levels of impulsivity caused a small but significant increase in avoidance motivation. Given our moderately large sample size, one should interpret the .047 p-value with care. Depending on the underlying impetus for the impulsive motivation to act, the results could suggest that impulsivity is either functional or dysfunctional in this particular model. Functional impulsivity might spur a highly competent subject to action, while dysfunctional impulsivity might lead to action when the subject has insufficient skill or has given the action insufficient forethought. More research needs to determine whether the effects of impulsivity are functional or dysfunctional in the extant model.

Overall, the results of the expanded model effectively account for a substantially larger percentage of the variance in avoidance behavior compared to any previous study. We achieved this result using a large, demographically diverse sample relative to past TTAT replication studies. Moreover, the depth and breadth of the data allows one to interpret and apply the results across organization type and geography. Self-efficacy was insignificant in our study, which raises concerns about this measure's continued use. Due to inconsistencies across multiple studies, we scrutinized the self-efficacy items and believe this construct requires revision to provide a clearer focus on security-specific forms of self-efficacy to be relevant in this domain.

6.1 Contributions

This paper makes several contributions to TTAT theory and has implications for security practitioners. First, we put forth a potential explanation for why prior TTAT empirical tests have yielded mixed results—particularly in terms of the influence of susceptibility and severity on threat perceptions. Additionally, we provide an alternative model that we believe provides better explanatory value of the threat-assessment process. In addition, we extend the TTAT model to account for individual differences that influence threat perceptions, avoidance motivation levels, and behavior. We tested our proposed model using a large sample that we collected from a set of highly heterogeneous individuals, which reinforces the theory's generalizability. Our results lend support for TTAT's generalizability. Finally, we mindfully chose our sample size to ensure that

we achieved significant statistic power to detect small Cohen effect sizes, which ensures that we robustly tested the influence of each construct in our revised TTAT model (Cohen, 1992).

In terms of practice, our findings provide several insights concerning how avoidance motivation decisions occur. Security practitioners can use this information to craft policies, messages, and education programs to enhance individuals' motivations to behave more securely. Our first insight concerns messaging regarding safeguard effectiveness. An individual's belief in the effectiveness of a security safeguard plays a key motivating role in whether the individual adopts the safeguard. In fact, both we and Liang and Xue (2010) found that safeguard effectiveness had the largest positive influence on avoidance motivation. Accordingly, we believe that security practitioners must do a better job at marketing the effectiveness of security measures to their constituents. Security policies and messages should not only state how users should behavior but also explain the efficacy and importance of the recommended safeguard measures.

Our second key insight concerns improving individuals' beliefs regarding their ability to implement and use security safeguards. Liang and Xue (2010) found support for a positive association between one's beliefs about one's ability to implement a security safeguard and avoidance motivation, which makes perfect sense since individuals will be motivated to do something if the feel confident in their ability to do so. However, in our sample, we did not find support for a significant association between such beliefs and our respondents' motivation to install and use security software to avoid malware. This difference is unsettling because it indicates that, in our sample, individuals who felt confident in their ability to use security software had no more motivation to install and use it than individuals who lacked confidence in their abilities. The difference between Liang and Xue's (2010) results and ours may actually have resulted from time and changes in the security landscape. Since 2010, numerous major security compromises have occurred, and the media has widely discussed several new types of security exploits. As such, competent individuals may lack motivation use security software because they do not feel that their actions really matter. Security practitioners must face this challenge head on and first make sure that the safeguards they design are simple and straightforward to use so that all users feel more confident in their abilities. Additionally, as we mention above, security practitioners must clearly explain the effectiveness of the proposed safeguard and the impact that adoption and use have on the broader security landscape.

Our next key insight involves the influence of risk propensity and impulsivity in individual's security avoidance decisions. In our sample, increased risk propensity was associated with a reduced level of threat perception and heightened impulsivity was associated with an increase in avoidance motivation. As such, security practitioners need to ensure that constituents appreciate the numerous threats present and motivate them to behave in a secure fashion. To aid in this endeavor, companies could measure employees' risk propensity and impulsivity levels and use the results to customize security messages and training specifically for individuals with specific levels of risk propensity and impulsivity.

Finally, our last key insight concerns reducing individuals' perceptions about the level of effort they need to implement security safeguards. In both our and Liang and Xue's (2010) models, the effort cost associated with implementing a security safeguard was negatively associated with implementing the target safeguard. This finding is logical and straightforward. Individuals will not have motivation to behave in a secure manner if they perceive the target behavior as too challenging or strenuous. Again, this finding indicates that security professionals must ensure that all recommended safeguards are easy and straightforward for users to implement and use. We believe that cyber security technology vendors and policy writers can use these insights concerning safeguard effectiveness, self-efficacy, risk propensity, impulsivity, and effort cost to develop products, processes, and messages that more effectively encourage avoidance behavior.

6.2 Limitations and Future Research

As with all research, one needs to interpret our findings while considering the limitations of the study design and the research method we employed. While we strove to gather the data for this study from a highly heterogeneous, large sample of respondents, we acknowledge that problems could exist with using Amazon Mechanical Turk as the sole basis for our sample frame. The system is still relatively new, and Amazon Mechanical Turk workers could possibly systemically differ from other groups of Internet users regarding security concerns. Accordingly, future research efforts should test the refined TTAT model in other domains and industries in order to control for any potential biases that arise from our using Amazon Mechanical Turk for our sampling system.

We also acknowledge that we collected all of the constructs assessed in our study using self-reported measures. Prior research has shown that differences often exist between self-reported measures and actual

values. Accordingly, we note that our proposed refinement of TTAT builds on individuals' perceptions of cyber security motivations and behavior rather than their actual motivations and behaviors. Additionally, we note that we made several changes to Liang and Xue's (2010) TTAT instrument in order to improve the clarity of our survey questions. These changes included modifying the TTAT items' wording to better fit the malware context, making scaling changes so that we consistently used a seven-point Likert scale throughout the instrument, and dropping one of the perceived susceptibility items that prior TTAT studies have used. While we feel confident that our measures exhibited adequate levels of reliability and validity to support our findings, these instrument changes could have resulted in slightly different interpretations of the TTAT constructs. Finally, we must note that we did not provide a specific definition of malware in the survey instructions, which we acknowledge may have resulted in respondents' applying differing interpretations when completing the survey and, thus, affected our results. Additionally, although a power analysis indicated that we needed 647 responses to detect small Cohen's f2 effect sizes (Rice & Harris, 2005) with our research model, we ended up with only 644 valid survey responses. Our slightly smaller than recommended sample has only one practical effect: that one could question our finding regarding self-efficacy being a non-significant predictor of avoidance behavior. However, given that our results with a sample size of 644 responses did not approach significance, it seems unlikely that the results would have changed with a small number of additional responses. Our sample size limitation may have been more important if more insignificant findings existed or if the single non-significant relationship had approached significance.

One opportunity to extend the TTAT literature involves enhancing measurement of the core TTAT constructs. Several individual items in the original Liang and Xue (2010) instrument assess multiple disparate constructs, which makes the meaning of the respondent's answer unclear. For example, for our study, we adopted Liang and Xue's item "I don't have anti-spyware on my PC because I don't know how to get an anti-spyware software" and revised it to "I don't have security software on my PC because I don't know how to get it". Both these items individually ask two different and distinct questions (i.e., 1) do you have threat-mitigating software on your PC and 2) do you know how to get threat-mitigating software), which respondents may find confusing. Accordingly, we recommend that future researchers carefully examine the text of all TTAT items in order to clarify their meaning. Additionally, Liang and Xue's (2010) instrument uses 10 items to measure several of the core constructs. We believe this high number of questions may contribute to survey exhaustion and result in some respondents dropping out of the survey before completion. Accordingly, researchers should develop a more parsimonious yet robust TTAT instrument.

We did not find support for the hypothesis about the influence of self-efficacy on avoidance motivation. While this result concurs with what previous researchers have found, the strong theoretical basis for self-efficacy as a predictor of IT behaviors begs for additional exploration regarding this relationship. In conducting such an exploration, one may need to carefully examine each self-efficacy item to determine its suitability in the specific context of the particular study. Additionally, note that one of the self-efficacy items loaded slightly below the 0.70 level and another item loaded just at 0.70, which further indicates that efforts to explore the self-efficacy/avoidance motivation relationship should focus on improving measurement of the self-efficacy construct.

Finally, researchers need to conduct supplemental work to fully understand the relationship between impulsivity and avoidance motivation. While we found support for an association, the influence was in the opposite direction of our original hypothesis. This finding means that, for our sample, more impulsive individuals had more motivation to avoid malware threats. We note that the impulsivity scales that TTAT studies most commonly use do not distinguish between functional and dysfunctional impulsivity as researchers commonly model in the psychology literature (Jones & Paulhus, 2011), which may cause counteracting influences where the two types of impulsivity have opposite effects and reduce the significance when modeled as a single variable. Note that the significance of the association was 0.047, close to the 0.05 level commonly used to assess statistical significance. Accordingly, we need a robust replication to shed light on this relationship.

7 Conclusion

Our refining the technology threat avoidance theory yielded positive results—particularly in the area of resolving the susceptibility, severity, and threat inconsistencies in previous work. Support for the theory in general coupled with construct refinement and validation of improved items provides an interesting story. The continued failure of general self-efficacy measures strongly indicates the need to develop a technology-based self-efficacy scale more suitable for use in the technology threat behavior domain. This exploration may require one to carefully examine each self-efficacy item. Overall, our study provides substantial insights

and refinement to the theory base on threat avoidance behavior. We believe these refinements will benefit future research and provide practitioners with better tools to elicit compliance with security policies and best practices.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. A., & Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, *1*(1), 69-79.

Abrantes, A. M., Strong, D. R., Lejuez, C. W., Kahler, C. W., Carpenter, L. L., Price, L. H., Niaura, R., & Brown, R. A. (2008). The role of negative affect in risk for early lapse among low distress tolerance smokers. *Addictive Behaviors*, *33*(11), 1394-1401.

Aguinis, H., & Lawal, S. O. (2012). Conducting field experiments using eLancing's natural environment. *Journal of Business Venturing*, *27*(4), 493-505.

Amazon. (2008). *Amazon Mechanical Turk launches new Web-based tools that bring the power of an on-demand workforce to businesses worldwide*. Retrieved from https://press.aboutamazon.com/news-releases/news-release-details/amazon-mechanical-turk-launches-new-web-based-tools-bring-power

Amir, N., Kuckertz, J. M., & Najmi, S. (2013). The effect of modifying automatic action tendencies on overt avoidance behaviors. *Emotion*, *13*(3), 478-484.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411-423.

Appelt, K. C., Milch, K. F., Handgraaf, M. J., & Weber, E. U. (2011). The decision making individual differences inventory and guidelines for the study of individual differences in judgment and decision-making research. *Judgment and Decision Making*, *6*(3), 252-262.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Ashleigh, M., Higgs, M., & Dulewicz, V. (2012). A new propensity to trust scale and its relationship with individual well-being: Implications for HRM policies and practices. *Human Resource Management Journal*, *22*(4), 360-376.

Bari, A., & Robbins, T. W. (2013). Inhibition and impulsivity: Behavioral and neural basis of response control. *Progress in Neurobiology*, *108*, 44-79.

Benamati, J., & Serva, M. A. (2007). Trust and distrust in online banking: Their role in developing countries. *Information Technology for Development*, *13*(2), 161-175.

Bendoly, E., Donohue, K., & Schultz, K. L. (2006). Behavior in operations management: Assessing recent findings and revisiting old assumptions. *Journal of Operations Management*, *24*(6), 737-752.

Boysen, S., McLeod, A., & Hewitt, B. (2017). *Modifying the technology threat avoidance theory* (Unpublished Master's Thesis). Texas State University, New Braunfels.

Brandstätter, V., Lengfelder, A., & Gollwitzer, P. M. (2001). Implementation intentions and efficient action initiation. *Journal of Personality and Social Psychology*, *81*(5), 946-960.

Broos, N., Schmaal, L., Wiskerke, J., Kostelijk, L., Lam, T., Stoop, N., Weierink, L., Ham, J., de Geus, E. J. C., Schoffelmeer, A. N. M., van den Brink, W., Veltman, D. J., de Vries, T. J., Pattij, T., & Goudriaan, A. E. (2012). The relationship between impulsive choice and impulsive action: A cross-species translational study. *PloS One*, *7*(5), e36781.

Browne, S., Lang, M., & Golden, W. (2015). Linking threat avoidance and security adoption: A theoretical model for SMEs. In *Proceedings of the 28th Bled eConference.* Retrieved from https://domino.fov.uni-mb.si/proceedings.nsf/Proceedings/6DC83D3888DEC65BC1257E5B0046BAB5/$File/3_Browne.pdf

Bujang, Y. R., & Hussin, H. (2012). Investigating email users behavior against spam: A proposed theoretical framework. *Journal of Internet and E-Business Studies*. Retrieved from https://ibimapublishing.com/articles/JIEBS/2012/264305/936368.pdf

Casler, K., Bickel, L., & Hackett, E. (2013). Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-face behavioral testing. *Computers in Human Behavior*, *29*(6), 2156-2160.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, *40*(1), 205-222.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447-459.

Cheung, J. H., Burns, D. K., Sinclair, R. R., & Sliter, M. (2017). Amazon Mechanical Turk in organizational psychology: An evaluation and practical recommendations. *Journal of Business and Psychology*, *32*(4), 347-361.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, *295*(2), 295-336.

Churchill, S., & Jessop, D. (2010). Spontaneous implementation intentions and impulsivity: Can impulsivity moderate the effectiveness of planning strategies? *British Journal of Health Psychology*, *15*(3), 529–541.

Cloninger, C. R., Przybeck, T. R., & Svrakic, D. M. (1991). The tridimensional personality questionnaire: US normative data. *Psychological Reports*, *69*(3), 1047-1057.

Cohen, J. (1988). *Statistical power analyses for the social sciences.* Hillsdale, NJ: Lawrence Erlbauni Associates.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155-159.

Couraud, J. R. (2014). *Risk perception in online communities* (doctoral thesis). Retrieved from http://digitalcommons.usu.edu/etd/3898/

Dalley, J. W., Everitt, B. J., & Robbins, T. W. (2011). Impulsivity, compulsivity, and top-down cognitive control. *Neuron*, *69*(4), 680-694.

D'Arcy, J., & Hovav, A. (2004). The role of individual characteristics on the effectiveness of IS security countermeasures. In *Proceedings of the Americas Conference on Information Systems.*

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

De Wit, H. (2009). Impulsivity as a determinant and consequence of drug use: A review of underlying processes. *Addiction Biology*, *14*(1), 22-31.

Einhorn, H. J. (1970). The use of nonlinear, noncompensatory models in decision making. *Psychological Bulletin*, *73*(3), 221-230.

Eysenck, H. J., & Eysenck, M. W. (1985). *Personality and individual differences: A natural science approach.* New York, NY: Plenum.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149-1160.

Gefen, D., Rigdon, E. E., & Straub, D. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, *35*(2), iii-A7.

Ghosh, D. (1994). Tolerance for ambiguity, risk preference, and negotiator effectiveness. *Decision Sciences*, *25*(2), 263-280.

Granö, N., Virtanen, M., Vahtera, J., Elovainio, M., & Kivimäki, M. (2004). Impulsivity as a predictor of smoking and alcohol consumption. *Personality and Individual Differences*, *37*(8), 1693-1700.

Grasmick, H., Tittle, C. R., Bursik, B., & Arneklev, B. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, *30*(1), 5-29.

Guarino, B. (2016). How many full-time Mechanical Turks work for Amazon? Can you live at two cents a microjob? *Inverse.* Retrieved from https://www.inverse.com/article/7066-how-many-full-time-mechanical-turks-are-there

Harman, D. (1976). A single factor test of common method variance. *Journal of Psychology*, *35*, 359-379.

Hsiao, R. L. (2003). Technology fears: Distrust and cultural persistence in electronic marketplace adoption. *The Journal of Strategic Information Systems*, *12*(3), 169-199.

Hung, K. T., & Tangpong, C. (2010). General risk propensity in multifaceted business decisions: Scale development. *Journal of Managerial Issues*, *22*(1), 88-106.

Hung, K. T., Tangpong, C., Li, J., & Li, Y. (2012). Robustness of general risk propensity scale in cross-cultural settings. *Journal of Managerial Issues*, *24*(1), 78-96.

Jackson, D. N., Hourany, L., & Vidmar, N. J. (1972). A four-dimensional interpretation of risk taking. *Journal of Personality*, *40*(3), 483-501.

Jones, D. N., & Paulhus, D. L. (2011). The role of impulsivity in the dark triad of personality. Personality and Individual Differences, *51*(5), 679-682.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security Privacy*, *9*(3), 49-51.

Lauriola, M., & Levin, I. P. (2001). Relating individual differences in attitude toward ambiguity to risky choices. *Journal of Behavioral Decision Making*, *14*(2), 107-122.

Lee, J., Ahn, J. H., & Park, B. (2015). The effect of repetition in Internet banner ads and the moderating role of animation. *Computers in Human Behavior*, *46*, 202-209.

Levin, I. P., Weller, J. A., Pederson, A. A., & Harshman, L. A. (2007). Age-related differences in adaptive decision making: Sensitivity to expected value in risky choice. *Judgment and Decision Making*, *2*(4), 225-233.

Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998). Trust and distrust: New relationships and realities. Academy of Management Review, *23*(3), 438-458.

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.

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

Lin, C. H., Shih, H. Y., & Sher, P. J. (2007). Integrating technology readiness into technology acceptance: The TRAM model. *Psychology & Marketing*, *24*(7), 641-657.

Lipton, E., Sanger, D. E., & Shane, S. (2016). The perfect weapon: How Russian cyberpower invaded the U.S. *The New York Times.* Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Manzano, D. L. (2012). The cybercitizen dimension: A quantitative study using a threat avoidance perspective. Capella University. Retrieved from http://search.proquest.com/openview/9e83e1d6a0859bbefab8787a07db1cf0/1?pq-origsite=gscholar&cbl=18750&diss=y

McKnight, D. H., & Chervany, N. L. (2001). Trust and distrust definitions: One bite at a time. In R. Falcone, M. Singh, & Y. H. Tan (Eds.), *Trust in cyber-societies* (pp. 27-54). Berlin: Springer.

McKnight, D. H., & Choudhury, V. (2006). Distrust and trust in B2C e-commerce: Do they differ? In *Proceedings of the 8th International Conference on Electronic Commerce* (pp. 482-491).

McKnight, H., Kacmar, C., & Choudhury, V. (2003). Whoops... Did I use the wrong concept to predict e-commerce trust? Modeling the risk-related effects of trust versus distrust concepts. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences.*

Menn, J. (2013). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters*. Retrieved from http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131221

Mohammed, S., & Schwall, A. (2009). Individual differences and decision making: What we know and where we go from here. *International Review of Industrial and Organizational Psychology*, *24*, 249-312.

Moody, G., Galletta, D., Walker, J., & Dunn, B. (2011). Which phish get caught? An exploratory study of individual susceptibility to phishing. In *Proceedings of the International Conference on Information Systems.*

Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In *Proceedings of the 47th Hawaii International Conference on System Sciences* (pp. 3188-3197).

Mwagwabi, F. (2015). *A protection motivation theory approach to improving compliance with password guidelines* (doctoral dissertation). Murdoch University.

Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, *39*(4), 865-892.

Nguyen, Q. N., & Kim, D. J. (2017). Enforcing information security protection: Risk propensity and self-efficacy perspectives. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 4747-4956).

Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research*, *8*(2), 157-176.

OWASP. (2017). *OWASP / Top10.* Retrieved from https://github.com/OWASP/Top10

Pablo, A. L. (1997). Reconciling predictions of decision making under risk: Insights from a reconceptualized model of risk behaviour. *Journal of Managerial Psychology*, *12*(1), 4-20.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Annual Hawaii International Conference on System sciences.*

Perry, J. L., & Carroll, M. E. (2008). The role of impulsive behavior in drug abuse. *Psychopharmacology*, *200*(1), 1-26.

Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, *99*(2), 33-42.

Preacher, K. J., & Leonardelli, G. J. (2001). *Calculation for the Sobel test: An interactive calculation tool for mediation tests (*computer software). Retrieved from http://quantpsy.org/sobel/sobel.htm

Rhoa, H., & Yub, I. (2011). The impact of information technology threat avoidance factors on avoidance behavior of user. Retrieved from https://pdfs.semanticscholar.org/a9e9/31b792c403f49a91a1dbdfdfbc34b92f1d8c.pdf

Rice, M. E., & Harris, G. T. (2005). Comparing effect sizes in follow-up studies: ROC area, Cohen's d, and r. *Law and Human Behavior*, *29*(5), 615-620.

Ross, J., Irani, I., Six, M., Zaldivar, A., & Tomlinson, B. (2010). Who are the crowdworkers? Shifting demographics in Amazon Mechanical Turk. In *Proceedings of Conference on Human Factors in Computing Systems* (pp. 2863-2872).

Ryan, D. J., & Heckman, C. (2003). Two views on security software liability: Let the legal system decide. *IEEE Security & Privacy*, *99*(1), 70-72.

Salvagnini, P., Bazzani, L., Cristani, M., & Murino, V. (2013). Person re-identification with a PTZ camera: An introductory study. In *Proceedings of the 20th IEEE International Conference on Image Processing* (pp. 3552-3556).

Schreiber, L. R., Grant, J. E., & Odlaug, B. L. (2012). Emotion regulation and impulsivity in young adults. *Journal of Psychiatric Research*, *46*(5), 651-658.

Schumann, A., & Monari, E. (2014). A soft-biometrics dataset for person tracking and re-identification. In *Proceedings of the 11th IEEE International Conference on Advanced Video and Signal Based Surveillance* (pp. 193-198).

Schweizer, K. (2002). Does impulsivity influence performance in reasoning? *Personality and Individual Differences*, *33*(7), 1031-1043.

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized casual inference.* Boston: Houghton Mifflin Company.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In *Proceedings of the International Information Security Conference* (pp. 133-144).

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. *Academy of Management Review*, *17*(1), 9-38.

Sitkin, S. B., & Roth, N. L. (1993). Explaining the limited effectiveness of legalistic "remedies" for trust/distrust. *Organization Science*, *4*(3), 367-392.

Sitkin, S. B., & Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management Journal*, *38*(6), 1573-1592.

Smith, M., & Green, M. (2016). *A discussion of surveillance backdoors: Effectiveness, collateral damage and ethics.* Retrieved from http://mattsmith.de/pdfs/SurveillanceAndCollateralDamage.pdf

Spiezle, C., & Wilbur, J. (2017). *2017 cyber incident & breach response briefing.* Washington, DC: Online Trust Alliance. Retrieved from https://otalliance.org/system/files/files/resource/documents/2017dpd.pptx.pdf

Sun, J., & Ahluwalia, P. (2008). How users respond to authentication methods: A study of security readiness. In *Proceedings of the Americas Conference on Information Systems.*

Sun, Y., & Upadhyaya, S. (2015). Secure and privacy preserving data processing support for active authentication. *Information Systems Frontiers*, *17*(5), 1007-1015.

Tice, D. M., Bratslavsky, E., & Baumeister, R. F. (2001). Emotional distress regulation takes precedence over impulse control: If you feel bad, do it! *Journal of Personality and Social Psychology*, *80*(1), 53-67.

Vance, A., Anderson, B. B., Kirwan, C. B., & Earle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*(10), 679-722.

Vilares, M., Almeida, M., & Coelho, P. (2010). Comparison of likelihood and PLS estimators for structural equation modeling: A simulation with customer satisfaction data. In V. E. Vinzi, W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of partial least squares: Concepts, methods and applications*. Berlin: Springer.

Weber, E. U. (2001). Personality and risk taking. In N. J. Smelser & P.B. Baltes (Eds.), *International encyclopedia of the social and behavioral sciences* (vol 11, pp. 11274). Amsterdam: Elsevier.

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.

WikiLeaks. (2016). *Search the DNC email database.* Retrieved from https://wikileaks.org/dnc-emails/

Wilkinson, L. (1999). Statistical methods in psychology journals: Guidelines and explanations. *American Psychologist*, *54*(8), 594-604.

Williams, J. (2017). New OWASP top 10 reveals critical weakness in application defenses. *Dark Reading*. Retrieved from http://www.darkreading.com/application-security/new-owasp-top-10-reveals-critical-weakness-in-application-defenses/a/d-id/1328751

Xue, Y., Liang, H., Mbarika, V., Hauser, R., Schwager, P., & Getahun, M. K. (2015). Investigating the resistance to telemedicine in Ethiopia. *International Journal of Medical Informatics*, *84*(8), 537-547.

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research*, *2*(6), 1-17.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information* Systems, *16*(6), 448-484.

Zetter, K. (2009). Senate panel: 80 percent of cyber attacks preventable. *Wired.* Retrieved from https://www.wired.com/2009/11/cyber-attacks-preventable/

Zhang, X., Prybutok, V. R., & Strutton, D. (2007). Modeling influences on impulse purchasing behaviors during online marketing transactions. *Journal of Marketing Theory and Practice*, *15*(1), 79-89.

Appendix

Table A1. Instrument

Construct	Indicator	Indicator text
Perceived susceptibility	SUS1	It is extremely likely that my computer will contain malware in the future.
	SUS2	The chances of getting malware on my system are great.
	SUS3	There is a good possibility that my computer will contain malware at some point.
	SUS4	There is a good chance that there will be malware on my computer at some point in the future.
Perceived severity	SEV1	Malware could steal personal information from my computer without my knowledge.
	SEV2	Malware could invade my privacy.
	SEV3	My personal information collected by malware could be misused by cyber criminals.
	SEV4	Malware could record my Internet activities and send it to unknown parties.
	SEV5	My personal information collected by malware could be subjected to unauthorized secondary use.
	SEV6	My personal information collected by malware could be used to commit crimes against me.
	SEV7	Malware could slow down my Internet connection.
	SEV8	Malware could make my computer run more slowly.
	SEV9	Malware could cause my systems to crash from time to time.
	SEV10	Malware could affect some of my computer programs and make them difficult to use.
Perceived threat	THR1	Malware poses a threat to me.
	THR2	The consequences of getting malware on my computer threaten me.
	THR3	Malware is a danger to my computer.
	THR4	It would be dreadful if my computer was infected by malware.
	THR5	It would be risky to use my computer if it had malware.
Perceived effectiveness	EFF1	Computer security software would be useful for detecting and removing malware.
	EFF2	Computer security software would increase my ability to protect my computer from malware.
	EFF3	Computer security software would enable me to search and remove malware on my computer faster.
	EFF4	Computer security software would enhance my effectiveness in finding and removing malware on my computer.
	EFF5	Computer security software would make it easier to search for and remove malware on my computer.
	EFF6	Computer security software would increase my productivity in searching and removing malware on my computer.
Safeguard cost	CST1	I don't have security software on my computer because I don't know how to get it.
	CST2	I don't have security software on my computer because it may cause problems with other programs on my computer
	CST3	I don't have security software on my computer because installing it is too much trouble.
Self-efficacy	SEF1	I could successfully install and use computer security software if there was no one around to tell me what to do.
	SEF2	I could successfully install and use computer security software if I had never used a package like it before.
	SEF3	I could successfully install and use computer security software if I only had the software manuals for reference.
	SEF4	I could successfully install and use computer security software if I had seen someone else do it before trying myself.

Table A1. Instrument

	SEF5	I could successfully install and use computer security software if I could call someone for help if I got stuck.
	SEF6	I could successfully install and use computer security software if someone helped me get started.
	SEF7	I could successfully install and use computer security software if I had a lot of time to complete the task.
	SEF8	I could successfully install and use computer security software if I only had the built-in help facility for assistance.
	SEF9	I could successfully install and use computer security software if someone showed me how to do it first.
	SEF10	I could successfully install and use computer security software if I had used a similar package before.
Avoidance motivation	MOT1	I intend to use computer security software to avoid malware breaches.
	MOT2	I use computer security software to avoid malware breaches.
	MOT3	I plan to use computer security software to avoid malware.
Avoidance behavior	BEH1	I run computer security software regularly to remove malware from my computer.
	BEH2	I update my computer security software regularly.
Risk propensity	RSK1	I engage in risky recreational activities (e.g., rock-climbing, scuba diving)
	RSK2	I engage in risky health related behaviors (e.g., smoking, poor diet, high alcohol consumption)
	RSK3	I engage in risky career related behaviors (e.g., quitting a job without another to go to)
	RSK4	I take safety risks (e.g., fast driving, cycling without a helmet)
	RSK5	I take financial risks (e.g., gambling, risky investments)
	RSK6	I take social risks (e.g., standing for election, publicly challenging rules or decisions)
Impulsivity	IMP1	I often act on the spur of the moment without stopping to think.
	IMP2	I don't devote much thought and effort to preparing for the future.
	IMP3	I often do whatever brings me pleasure here and now, even at the cost of distant goals.
	IMP4	I'm more concerned with what happens to me in the short run than in the long run.

Table A2. Factor Loadings

	SUS	SEV	RSK	DIST	THR	EFF	COS	SEF	IMP	MOT	BEH
SUS1	**0.92**	0.30	0.10	0.13	0.33	0.22	0.06	-0.08	0.11	0.17	0.14
SUS2	**0.87**	0.28	0.12	0.14	0.34	0.20	0.13	-0.07	0.17	0.13	0.10
SUS3	**0.90**	0.39	0.05	0.13	0.36	0.28	0.00	-0.02	0.08	0.23	0.19
SUS4	**0.92**	0.36	0.07	0.12	0.36	0.27	0.00	-0.03	0.06	0.18	0.15
SEV1	0.33	**-0.83**	0.10	0.17	0.57	0.52	0.27	-0.20	0.14	0.36	0.28
SEV2	0.29	**-0.86**	0.14	0.21	0.63	0.56	0.34	-0.24	0.20	0.39	0.30
SEV3	0.30	**-0.85**	0.10	0.19	0.59	0.53	0.31	-0.21	0.16	0.39	0.31
SEV4	0.29	**-0.82**	0.10	0.16	0.53	0.48	0.31	-0.25	0.16	0.33	0.28
SEV5	0.32	**-0.86**	0.14	0.16	0.58	0.53	0.35	-0.18	0.18	0.35	0.28
SEV6	0.29	**-0.77**	0.09	0.16	0.54	0.44	0.26	-0.18	0.16	0.29	0.25
SEV7	0.29	**-0.76**	0.08	0.11	0.50	0.46	0.30	-0.14	0.18	0.33	0.29
SEV8	0.28	**-0.80**	0.15	0.19	0.52	0.52	0.35	-0.17	0.20	0.37	0.30
SEV9	0.32	**-0.76**	0.11	0.11	0.50	0.42	0.24	-0.15	0.18	0.29	0.23
SEV10	0.31	**-0.82**	0.16	0.17	0.53	0.49	0.33	-0.18	0.20	0.34	0.26
RSK1	-0.07	0.17	**0.83**	-0.12	-0.20	0.22	0.42	0.00	-0.47	-0.15	0.04
RSK2	-0.05	0.03	**0.65**	-0.14	-0.10	0.07	0.26	0.06	-0.44	-0.03	0.00
RSK3	-0.08	0.10	**0.77**	-0.17	-0.17	0.18	0.35	-0.04	-0.47	-0.17	0.12
RSK4	-0.11	0.07	**0.74**	-0.17	-0.11	0.12	0.35	-0.05	-0.48	-0.14	0.11
RSK5	-0.07	0.14	**0.80**	-0.12	-0.20	0.19	0.40	-0.04	-0.46	-0.12	0.06
RSK6	-0.05	0.09	**0.77**	-0.09	-0.14	0.19	0.34	0.03	-0.35	-0.14	0.03
DIST1	0.12	0.16	0.15	**0.85**	0.14	0.08	0.07	0.02	0.26	0.03	0.02
DIST2	0.11	0.09	0.19	**0.81**	0.12	0.00	0.18	0.04	-0.31	-0.08	0.08
DIST3	0.12	0.08	0.19	**0.78**	0.11	0.00	0.16	0.00	-0.35	-0.03	0.03
DIST4	0.09	0.18	0.13	**0.84**	0.15	0.13	0.07	0.06	0.28	-0.03	0.00
DIST5	0.13	0.25	0.09	**0.85**	0.28	0.22	0.01	0.05	0.17	0.14	0.11
THR1	0.40	-0.53	0.12	0.19	**0.83**	0.48	0.21	-0.13	0.15	0.42	0.31
THR2	0.38	-0.52	0.12	0.16	**0.80**	0.50	0.14	-0.16	0.10	0.31	0.24
THR3	0.33	-0.59	0.17	0.20	**0.81**	0.56	0.26	-0.19	0.19	0.41	0.31
THR4	0.24	-0.46	0.22	0.16	**0.75**	0.51	0.22	-0.14	0.15	0.38	0.28
THR5	0.18	-0.57	0.20	0.13	**0.76**	0.50	0.22	-0.25	0.18	0.34	0.27
EFF1	0.19	-0.50	0.21	0.12	0.54	**0.87**	0.36	-0.28	0.15	0.55	0.47
EFF2	0.27	-0.54	0.18	0.15	0.57	**0.86**	0.35	-0.30	0.16	0.56	0.46
EFF3	0.23	-0.54	0.19	0.11	0.56	**0.85**	0.33	-0.24	0.20	0.52	0.45
EFF4	0.24	-0.52	0.24	0.11	0.58	**0.85**	0.41	-0.26	0.19	0.60	0.50
EFF5	0.23	-0.53	0.15	0.13	0.55	**0.87**	0.36	-0.29	0.18	0.51	0.45
EFF6	0.24	-0.51	0.18	0.06	0.52	**0.84**	0.30	-0.24	0.15	0.46	0.38
CST1	-0.07	0.36	0.40	-0.06	-0.25	0.32	**0.86**	-0.11	-0.42	-0.39	0.38
CST2	-0.04	0.31	0.41	-0.10	-0.21	0.39	**0.89**	-0.12	-0.43	-0.48	0.43
CST3	-0.04	0.35	0.44	-0.08	-0.26	0.38	**0.91**	-0.16	-0.43	-0.45	0.45
SLF1	0.07	0.18	0.05	0.01	0.13	0.18	0.08	**-0.69**	0.04	0.15	0.15
SLF3	0.08	0.14	0.02	0.03	0.13	0.22	0.09	**-0.73**	0.04	0.13	0.11
SLF4	0.08	-0.13	0.00	0.04	0.12	0.22	0.11	**-0.85**	0.07	0.16	0.12

Table A2. Factor Loadings

SLF5	0.03	-0.21	0.07	0.02	0.21	0.32	0.16	**-0.79**	0.13	0.21	0.18
SLF6	0.03	-0.12	0.03	0.03	0.14	0.22	0.10	**-0.80**	0.06	0.14	0.10
SLF7	0.02	-0.16	0.01	0.06	0.18	0.24	0.10	**-0.75**	0.09	0.19	0.12
SLF8	0.02	0.19	0.00	0.06	0.16	0.24	0.11	**-0.73**	0.07	0.16	0.17
SLF9	0.08	-0.11	0.04	0.00	0.14	0.19	0.09	**-0.82**	0.09	0.16	0.10
SLF10	0.03	-0.30	0.08	0.06	0.27	0.35	0.21	**-0.78**	0.15	0.28	0.22
IMP1	-0.14	0.17	0.57	-0.26	-0.16	0.16	0.42	-0.13	**-0.86**	-0.19	0.12
IMP2	-0.06	0.22	0.41	-0.19	-0.19	0.19	0.41	-0.04	**-0.80**	-0.17	0.14
IMP3	-0.06	0.16	0.47	-0.30	-0.17	0.17	0.38	-0.11	**-0.85**	-0.17	0.13
IMP4	-0.11	0.14	0.41	-0.29	-0.08	0.08	0.34	-0.04	**-0.75**	-0.08	0.07
MOT1	0.21	-0.39	0.15	0.03	0.45	0.59	0.45	-0.23	0.19	**0.95**	0.75
MOT2	0.16	-0.38	0.14	0.05	0.40	0.56	0.49	-0.18	0.18	**0.92**	0.82
MOT3	0.19	-0.41	0.18	0.06	0.47	0.60	0.46	-0.24	0.20	**0.94**	0.72
BEH1	0.17	-0.33	0.09	0.02	0.35	0.52	0.45	-0.18	0.15	0.78	**0.95**
BEH2	0.13	-0.32	0.06	0.03	0.33	0.48	0.44	-0.17	0.13	0.78	**0.94**

About the Authors

Darrell Carpenter is the Director of the Center for Cyber Security and an Assistant Professor of Information Systems and Cyber Security at Longwood University in Virginia. His primary research interests include behavioral and organizational aspects of systems security including acceptance / rejection of security technologies, motivations for engaging in risky online behavior, and on-line deception. He is also interested in information privacy, technology adoption/continuance behaviors, and inter-organizational benefits/effects of information systems. His research is published academic outlets including *Information Systems Frontiers, Information & Management, the Journal of Computer Information Systems, Computers in Human Behavior, Communications of the Association of Information Systems, the Association for Information Systems Transactions on Replication Research, and the International Journal of Information Management.*

Diana K. Young is an assistant professor at Trinity University in San Antonio, TX. She earned her doctorate in Information Technology from the University of Texas at San Antonio. Her research has been published in the *Journal of Computer Information Systems, the Association for Information Systems Transactions on Replication Research, and the Communications of the Association for Information Systems*. Her research interest include issues concerning behavior cyber security, IT data analytics workforce, and health information systems. Beyond her academic pursuits, she possesses over 20 years of practical IT experience.

Paul Barrett is a Professor in the Management program and former Dean of the College of Business and Economics at Longwood University in Farmville, Virginia. He was an important leader in multiple successful technology start-up companies, including one that evolved into a USA Securities Exchange Commission publicly traded corporation. In addition to his academic commitments, he remains engaged since 1992 in coaching global executives in the profit and non-profit worlds. He is consistently an invited speaker at national and global conferences and conventions. His research agenda includes cyber security, and organizational and leadership development.

Alexander McLeod is an Assistant Professor at Texas State University in the Health Information Management Department. He received his PhD in Information Technology from the University of Texas at San Antonio. Research interests include healthcare information systems, cyber security, cyber analytics, and ethics. He has published in the *Business Process Management Journal, Communications of the Association of Information Systems, CPA Journal, Decision Sciences Journal of Innovative Education, Decision Support Systems, Educational Perspectives in Health Informatics and Information Management, Fraud, Information Systems Frontiers, International Journal of Accounting Information Systems, International Journal of Biomedical Engineering and Technology, International Journal of Business Information Systems, International Journal of Electronic Healthcare, International Journal of Healthcare Information Systems and Informatics, Journal of Accounting Education, Journal of Business Ethics, Journal of Information Privacy and Security, Journal of Information Science and Technology, Journal of Information Systems Education, Perspectives in Health Information Management.*