Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Exploring the effect of uncertainty avoidance on taking voluntary protective security actions

Salvatore Aurigemma [a,*], *Thomas Mattson* [b]

[a] *University of Tulsa 800 South Tucker Drive, Helmerich Hall 313C, Tulsa, OK 74104, USA*
[b] *University of Richmond, 28 Westhampton Way, Richmond, Virginia*

ARTICLE INFO

Article history:
Received 4 September 2017
Accepted 1 November 2017
Available online 14 November 2017

Keywords:
Passwords
Password management
Hofstede
Uncertainty avoidance
Protection motivation theory
Password managers
Voluntary security actions

ABSTRACT

In this paper, we investigate the main and qualifying effect of Hofstede's uncertainty avoidance dimension (i.e., a culture's acceptance of ambiguous or uncertain situations) of national culture on an individual's protection motivation intentions (using protection motivation theory) to adopt an information security control voluntarily. Uncertainty avoidance is particularly relevant to protection motivation theory and voluntary security related actions, because individuals often perceive high levels of ambiguity related to the threat and the mitigating control that can be adopted voluntarily. The voluntary action that we investigated in this paper is the adoption of password managers due to the perceived uncertainty associated with the threat of having poor password management practices and the ambiguity related to the efficacy of adopting a password manager to mitigate this threat. Using a survey of 227 nationally diverse individuals, we found that uncertainty avoidance qualified the impact of perceived threat vulnerability and perceived threat severity on protection motivations to adopt a password manager voluntarily. In our data, the differential effect of uncertainty avoidance on perceived threat vulnerabilities was greater for those individuals reporting a below average level of uncertainty avoidance relative to an above average level of uncertainty avoidance, but we found the opposite qualifying effect on perceived threat severity. Counter to what we hypothesized, we found that the effect of uncertainty avoidance on protection motivations was negative. These results generally hold for the core and full PMT models. Our study suggests that a one-size fits all approach to security awareness education and training (especially for voluntary security actions) may not be appropriate due to the differential effect associated with individuals from different national cultures.

1. Introduction

Despite IBM's proclamation of the death of the password back in 2009, the password remains the primary defense mechanism used to protect an individual's online identity and digital assets (Ofcom, 2015). Information security professionals have preached (and continue to preach) ad nauseam about the importance of using sound password management practices such as not reusing passwords across multiple websites and using strong passwords (CSID, 2012). Unfortunately, individuals, for a variety of reasons, still consistently use poor password management practices. Within organizations, IT departments have the technical ability to mandate character minimums and character types (i.e., special characters, upper case, lower case, and so on) for passwords on their internal systems. However, individuals typically have accounts on many other websites (i.e., emails, banks, retail spaces, travel sites, and social media

* *Corresponding author.*
E-mail address: sal@utulsa.edu (S. Aurigemma).

https://doi.org/10.1016/j.cose.2017.11.001
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

accounts) outside the IT department's immediate control. At these other websites, individuals rarely (if ever) change their passwords, which is very problematic especially if the reused password is weak (Choong and Theofanos, 2015; Florencio and Herley, 2007; Stobert and Biddle, 2014).

One possible solution to this problem is to adopt a dedicated password manager application such as LastPass, KeePassX, and 1Password. A password manager application is encrypted software that securely stores all of an individual's passwords in a single location and, optionally, synchronizes all of an individual's passwords across multiple devices (Huth et al., 2013). Many leading security organizations such as SANS and US-CERT highly recommend the use of password manager applications as an important protection mechanism to guard against compromised passwords due to their usefulness in promoting sound password management practices (Huth et al., 2013; Zeltser, 2015). However, the use of password managers inside of organizations is still mostly optional and individuals' adopting these solutions outside of the work environment is entirely voluntary, which has resulted in very low adoption rates (Humphries, 2015).

Convincing individuals to adopt a voluntary information security control can be an onerous ordeal, especially if the voluntary action requires any amount of thought, organization, time, and energy to implement (Liang and Xue, 2010; Warkentin et al., 2016). Additionally, many voluntary information security actions require the individual to consciously or subconsciously make a risk assessment (i.e., threat, vulnerability, and exposure) and make the adoption decision partially based on that risk assessment (Boss et al., 2015; Posey et al., 2015). At least theoretically, this level of uncertainty (risk) should increase or decrease an individual's motivation to adopt the information security control voluntarily (Albrechtsen, 2007; Straub and Welke, 1998; van Schaik et al., 2017). For instance, when making a decision to adopt a password manager application voluntarily, individuals must assess the threat and negative impact of a compromised password. Information security professionals can encourage voluntary adoption by focusing on the seriousness of the threat and the negative consequences of not taking any protective measures to mitigate or manage the threat. However, certain individuals are inherently more comfortable with higher levels of risk and uncertainty than other individuals are (Chen et al., 2017; Chen and Zahedi, 2016).

Interestingly, individuals socialized in different national cultures have different levels of tolerance for uncertainty and ambiguity, which is referred to as uncertainty avoidance (Hofstede, 2001). Some cultures such as Singapore, Jamaica, and Denmark socialize their members to be comfortable with (and embrace) ambiguity whereas other cultures such as Greece, Portugal, and Guatemala socialize their members to seek certainty (i.e., avoid uncertainty). Therefore, given the importance of risk and uncertainty involved in making any voluntary information security decision, it would seem reasonable to predict that individuals socialized in different national cultures with varying tolerances for uncertainty would have different protection motivations and adoption rates. However, information security researchers have not investigated this conjecture theoretically or empirically, specifically related to password managers and other voluntary information security actions. Additionally, information systems researchers (more broadly than just security researchers) have consistently reported that the uncertainty avoidance cultural dimension is the most influential cultural dimension in explaining the variance in a variety of technology related phenomena (Cardon and Marshall, 2008; Straub, 1994; Sundqvist et al., 2005). Therefore, we address the following research question in our paper:

> **RQ**: What is the effect of uncertainty avoidance on motivations to adopt voluntary information security controls (specifically password manager applications)?

In order to answer this research question both theoretically and empirically, we build off and extend the protection motivation theory (PMT). We use the PMT because the PMT includes a threat appraisal mechanism and a coping mechanism, which makes it an attractive theory to explain voluntary security related actions and the impact of cross-cultural differences related to uncertainty and ambiguity. Specifically for voluntary information security actions, for instance, an individual typically must first assess the threat (i.e., poor password management practices) and then assess the veracity of the proposed coping mechanism (i.e., adopting a password manager) (Boss et al., 2015; Posey et al., 2015; Warkentin et al., 2016). However, neither the main nor qualifying effect of uncertainty avoidance have been empirically or theoretically investigated in PMT related research, but the correlation between risk and the uncertainty avoidance cultural construct makes this construct a logical extension to the PMT. Furthermore, using the PMT allows us to determine the incremental impact that uncertainty avoidance has beyond the common factors that prior researchers have already reported in the prior literature. To test the impact of uncertainty avoidance within the PMT empirically, we surveyed a culturally diverse sample of 227 individuals. In our sample, we found that the differential effect of uncertainty avoidance on perceived threat vulnerabilities was greater for those individuals reporting a below average level of uncertainty avoidance relative to an above average level of uncertainty avoidance, but we found the opposite qualifying effect on perceived threat severity. These results generally hold for both the core and the full PMT.

2. Theoretical foundations

There is not a universally accepted "correct" theory that explains the majority of the variance in information security behaviors (voluntary or mandatory). The existing literature has relied on a number of theories such as general deterrence theory (GDT), rational choice theory, social cognitive theory, the theory of planned behavior (TPB), psychological capital, and protection motivation theory (PMT) in order to explain why individuals perform (or not perform) a variety of information security related behaviors (Aurigemma, 2013; Crossler et al., 2013). For the past decade, scholars have debated the positives and negatives associated with each one of these theoretical approaches. Despite this debate, there is no consensus among behavioral information security researchers as to which theory is the most appropriate to use for a specific setting, sample, situation, and threat context in order to maximize the explained variance in

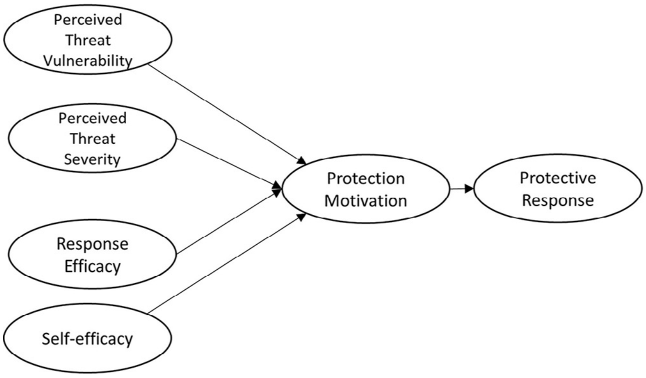

Fig. 1 – Core PMT Model as used by Warkentin et al. (2016).

adoption intentions, protection motivations, and actual behaviors. In our paper, we chose to use the PMT for the following reasons: 1) the logical connection between the uncertainty avoidance construct and the primary PMT constructs, 2) its applicability to voluntary information security actions (i.e., need to assess both the threat and the coping mechanism), and 3) the fact that the primary PMT constructs have typically been reported to be statistically significant in a variety of contexts with reasonable effect sizes (Herath and Rao, 2009; Warkentin et al., 2016).

2.1. *Protection motivation theory*

Although the PMT started out as a single theory when it was first formulated (Rogers, 1975, 1983), there are now many different variations of the PMT used in information security literature (and in other disciplines) (Crossler and Belanger, 2014; Herath and Rao, 2009; Johnston and Warkentin, 2010; Lee et al., 2008; Liang and Xue, 2010; Posey et al., 2013). However, there is certainly no universally accepted version of the PMT among the many different (equally valid) variants used in the information security literature.

Fig. 1 displays the core PMT in its most fundamental form. In this form, the PMT consists of four primary constructs: 1) an individual's self-efficacy to perform a security action (confidence in one's ability), 2) the perceived response efficacy of the required action (positive effects of the behavior), 3) the perception of the vulnerability from the related security threat (perceived likelihood that the threat will occur), and 4) the perceived severity of the security threat being studied (perceived impact of the threat) (Siponen et al., 2014; Warkentin et al., 2016). In general (with a few reported exceptions), existing literature has reported that higher self-efficacy, higher response efficacy, greater perceived vulnerabilities, and greater perceived severities are associated with increased protection motivations (behavioral intentions) to adopt information security controls (Crossler et al., 2014; Herath and Rao, 2009; Johnston and Warkentin, 2010; Johnston et al., 2015; Putri and Hovav, 2014; Wall et al., 2013; Warkentin et al., 2016; Workman et al., 2008).

Several information security researchers have extended the core PMT model to include additional constructs. For example, Workman et al. (2008) added locus of control in order to capture the proactive or reactive nature of the information security behavior. They theorized that an individual may have either an internal or an external locus of control, which may increase or decrease protection motivations. Crossler et al. (2014) added response cost (perception of the cost of performing a task) as an additional component of the PMT's coping appraisal to account for the differential costs in performing an information security action. In their PMT extension, high costs could be a deterrent to compliance intentions and protection motivations (Crossler et al., 2014). Boss et al. (2015) and Posey et al. (2015) further expanded the PMT to include perceived fear (based upon a specific fear-appeal impetus) and maladaptive rewards (a perceived benefit of not complying with the ISP). Their models specifically address using fear appeals to engender threats in order to motivate protective security behaviors. They specifically theorize that fear partially mediates core threat assessment constructs of perceived threat severity and vulnerability. According to these scholars, their model most closely resembles the theoretical origins of the original PMT. Fig. 2 displays their full PMT model.

However, to the best of our knowledge, PMT information security scholars have not investigated the direct, indirect, or qualifying effect of national culture, specifically the uncertainty avoidance dimension of national culture in any of the PMT models. This omission is significant because individuals socialized in different cultures develop different thought patterns, values, and culturally defined norms (Schein, 2010; Triandis, 1994), which may impact their protection motivations related to a variety of factors including voluntary information security controls. Furthermore, cross-cultural differences can influence how individuals respond to fear and form risk perceptions, which is directly related to the PMT and to the uncertainty avoidance dimension of national culture (Chen and Zahedi, 2016; Weber and Hsee, 2000).

2.2. *Culture*

Culture is often considered one of the primary driving forces behind human behavior in all different contexts, but culture is a concept that is difficult to define (Leidner and Kayworth, 2006; Triandis, 1994). For the past several decades, scholars have debated the definition of culture because it is such an abstract concept. Culture may be delimited and defined at (among others) the group, community, institution, occupation, industry, and national levels. In our paper, we define culture broadly as "the collective programming of the mind that distinguishes one group or category of people from another" (Hofstede and Bond, 1988, p. 51). Hofstede and Bond (1988) use this analogy to refer to different groups being programmed via social, political, educational, community, and economic means to process information and make sense of the world differently. By this logic, cultures develop shared values and norms through which individuals decide what actions are appropriate and inappropriate for a given situation (Schein, 2010).

Culture plays an important role in determining how groups of people are socialized to behave and think both individually and collectively (O'Reilly et al., 1991; Qiu et al., 2013). Dissimilar cultures have varying thought patterns and values along many dimensions, which provides individual members with a mind-set that is used to guide individual decision-making (Schein, 2010; Triandis, 1994). Said differently,

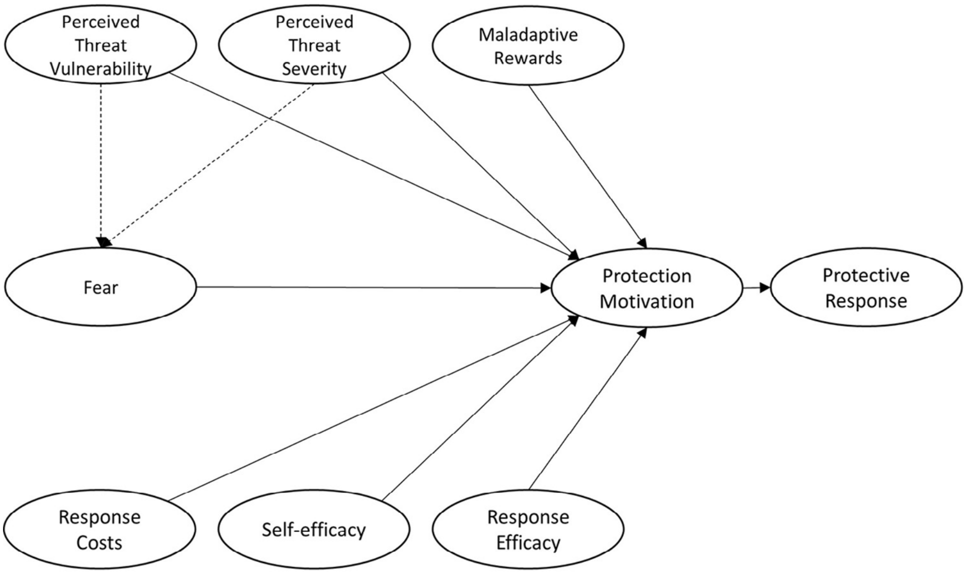

Fig. 2 – Full PMT proposed by Boss et al. (2015) and Posey et al. (2015).

socialization and conditioning within a culture provides the framework that individuals use in their everyday decision making processes. What is considered rational behavior in one culture may be considered irrational in another culture, because rational behaviors are based on what the culture defines and considers to be reasonable in a given context (Trompenaars and Hampden-Turner, 2011). How a culture defines norms is a complex process based on traditions, cultural institutions, events, and many different cultural characteristics and dimensions (Triandis, 1994).

Cultural theorists have determined that national cultures differ on many characteristics and dimensions. For example, Trompenaars and Hampden-Turner (2011), House et al. (2004), and Hall (1976) all theorized about national cultural differences related to communication styles, time orientation, relationships with space, the importance of rules and structures, and many other differences across cultures. However, information systems research has most commonly used Hofstede dimensions of national culture (power distance, uncertainty avoidance, individualism-collectivism, masculinity-femininity, long-term orientation, and indulgence) to measure and theorize about how national culture impacts technology related dependent variables (Kappos and Rivard, 2008; Leidner and Kayworth, 2006). Hofstede (2001) defines each dimension as follows: 1) power distance refers to the extent to which a culture accepts status inequalities; 2) uncertainty avoidance refers to a culture's acceptance of ambiguous or uncertain situations; 3) individualism-collectivism is the degree of interdependence a society maintains among its members; 4) masculinity-femininity refers to a cultures competitiveness such as wanting to be the best (masculinity) or caring for others (femininity); 5) long-term orientation refers to how a culture balances its past with the challenges of the present or future; and 6) indulgence refers to the extent to which a culture tries to control their impulses.

Within the information systems literature, scholars have investigated the impact of culture on a variety of IT and IS phenomena (Kappos and Rivard, 2008; Leidner and Kayworth, 2006; Veiga et al., 2001). For instance, prior information systems literature has reported cultural differences in systems design principles (Kankanhalli et al., 2004), the use of group design support systems (Daily et al., 1996), visualization in IS process models (Kummer et al., 2016), and general technology use (McCoy et al., 2007). The general conclusion across the different IS phenomena is that culture does impact a variety of IT related behaviors and developing a single theory that is applicable to all people in all cultures is highly problematic (Kappos and Rivard, 2008; Leidner and Kayworth, 2006). Interestingly, information systems researchers (more broadly than just security researchers) have consistently reported that the uncertainty avoidance cultural dimension is the most influential cultural dimension in explaining the variance in a variety of technology related phenomena (Cardon and Marshall, 2008; Straub, 1994; Sundqvist et al., 2005).

The behavioral information security literature has just recently started to investigate the role that cultural differences at the national level play in security related actions (Dinev et al., 2009; Dols and Silvius, 2010; Hovav, 2017; Hovav and D'Arcy, 2012; Karjalainen et al., 2013; Lowry et al., 2014). Initial findings in this area suggest that national culture is an important factor governing individuals' information security related actions. For instance, Hovav and D'Arcy (2012) explored the possible effect of national culture on employee information system misuse intention and found that there were significant differences in security intentions and behavioral antecedents between US and South Korean participants across a set of the same misuse scenarios. These studies, and others, have begun to examine and question the universality of human behaviors arguing that individuals from different national cultures can be expected to exhibit different information security related behaviors. Therefore, we need to further evaluate the effect of national culture on information security behaviors in order to best educate and inform security stakeholders (Karjalainen et al., 2013).

3. Research model

The uncertainty avoidance cultural dimension was developed specifically to address cross-cultural differences in uncertainty when making decisions (Hofstede, 2001), which makes it a logical extension to the PMT's threat and vulnerability components. The core idea behind this cultural dimension is that groups of people are socialized to have different levels of comfort with ambiguity and uncertainty. Individuals in different cultures are socialized to cope with and manage the anxiety associated with uncertainty differently. Certain cultures have a desire to minimize uncertainty whereas other cultures are not concerned with or even embrace uncertainty (Hofstede, 2001). There is not, however, a consensus view on how uncertainty avoidance (UA) as a cultural phenomenon affects an individual's acceptance of technologies. Whereas Hofstede suggests that those with high UA are more likely to welcome a technology that offers to reduce uncertainty (Cardon and Marshall, 2008), findings from technology-acceptance literature has investigated and found an opposite relationship. For example, Sundqvist et al. (2005) found that high UA cultures adopt new technologies slower, often waiting to learn from the experience of others that try the technology first. This is supported by other research that demonstrated that individuals from low uncertainty avoidance cultures tend to be more innovative and have a higher adoption rate of new technologies (Hermeking, 2005). This makes logical sense because low uncertainty avoidance cultures are more comfortable taking on risk and most technological adoption (at least related to brand new unproven technologies) decisions involve an unknown, risky element. Numerous other researchers have also concluded that higher UA cultures and individuals are more reluctant to try new technological solutions to existing needs or problems (Garfield and Watson, 1997; Hasan and Ditsa, 1999; Keil et al., 2000; Veiga et al., 2001).

The purpose of the fear appeal in the PMT is to create uncertainty surrounding the threat but certainty concerning the coping mechanism (or mitigating action) (Boss et al., 2015; Posey et al., 2015). In the case of password managers, an ideal fear appeal will prime individuals to be highly concerned about their poor password management practices while reducing the ambiguity associated with adopting password managers. Therefore, the focus of the uncertainty in the context of the PMT should be on the threat and not on the mature technology that is proposed to be adopted to mitigate that threat. In other theoretical perspectives such as the theory of planned behavior or the technology acceptance model, the focus of the uncertainty is on the technology and not the threat (Cardon and Marshall, 2008).

In our model, we assess that for information security issues with mature solutions, there will be a positive effect of UA on the intention to take the protective behavior. Password managers (and other common security technologies more broadly), are relatively mature technologies at this point. Therefore, these technologies represent a tried and tested approach to password management. If individuals have a low level of uncertainty avoidance (comfortable with ambiguity), then we predict that these individuals will have a reduced likelihood of adopting a password manager application because they are conceivably more comfortable with the uncertainty associated with having a password cracked or their account exposed due to password reuse on multiple accounts and platforms. However, and in keeping with Hoftsede's supposition on the effect of UA, we predict the opposite for those individuals with a high level of uncertainty avoidance, because these individuals will be more likely to adopt a tried and tested application (i.e., proven coping mechanism) in order to reduce the uncertainty associated with a specific threat (i.e., compromised account credentials). Therefore, we hypothesize the following main effect:

> **H1**: Individuals with a high uncertainty avoidance relative to a low uncertainty avoidance will have a greater protection motivation to adopt an information security control voluntarily, specifically password managers.

The two primary threat appraisal constructs in the PMT are perceived threat severity and perceived threat vulnerability. Both of these constructs have an element of uncertainty associated with their conceptual definitions. Therefore, we predict that uncertainty avoidance will qualify or otherwise moderate their impact on protection motivations to adopt a voluntary information security control (here, password manager applications). We suggest that this is the case because as the threat severity and vulnerability increase, the uncertainty avoidance dimension becomes activated or salient. This activation results in a heightened effect associated with high severity and high vulnerability threats due to these individuals having a low tolerance for ambiguity and risk. Park (1993) found that the penetration rate of life insurance policies is positively correlated with high uncertainty avoidance. Adopting a voluntary information security control is certainly conceptually similar to purchasing an optional insurance policy. Additionally, individuals with high levels of uncertainty have a greater faith in institutions (Lim et al., 2004), which may result in an enhanced effect for a fear appeal (especially if that fear appeal is coming from a highly reputable institution).

For those individuals with low levels of uncertainty avoidance, we suggest that the qualifying effect will be much flatter, possibly negative. The work of Keil et al. (2000) helps explain why we make this conjecture. They found that software project leaders were more likely to let a failing software project continue (i.e., escalation of commitment) if they were from a low uncertainty avoidance culture relative to a high uncertainty avoidance culture. In our context, this means that low uncertainty avoidance individuals might double down on the risk (i.e., continue to manually manage their weak passwords) when presented with a fear appeal related to poor password management and the benefits associated with adopting a password management application. Therefore, we hypothesize the following qualifying relationships:

> **H2**: An individual's level of uncertainty avoidance will qualify the effect of perceived threat vulnerability on their protection motivation to adopt an information security control voluntarily, specifically password managers.

> **H3**: An individual's level of uncertainty avoidance will qualify the effect of perceived threat severity on their protection

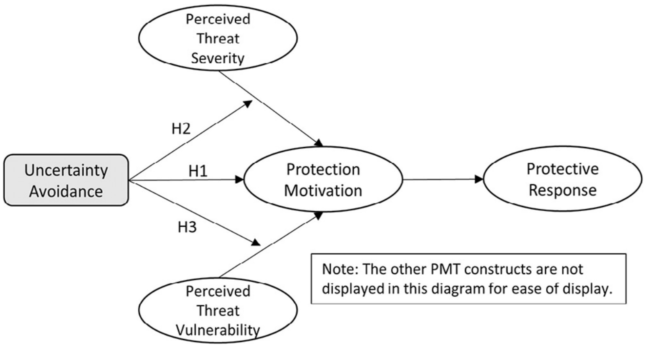
Perceived Threat Severity
Uncertainty Avoidance
H2
H1
H3
Protection Motivation
Protective Response
Perceived Threat Vulnerability
Note: The other PMT constructs are not displayed in this diagram for ease of display.

Fig. 3 – Research Model.

motivation to adopt an information security control voluntarily, specifically password managers.

Fig. 3 visually displays our research model.

4. Research design and method

To empirically test the potential impact of an individual's level of uncertainty avoidance on taking a voluntary information security action (adopting a password manager) in the context of the PMT, we conducted a two part study of the voluntary adoption (or non-adoption) of a password manager application (LastPass). We used LastPass because it is a well-respected password management application that uses industry-accepted encryption techniques to protect individuals' account credentials. It is also free so money was not a confounding variable in any type of protection motivation or adoption decision in our study. In part 1 of our study, we presented all participants with a video fear appeal threat message (available at https://www.youtube.com/watch?v=ru3JXo7YoVc). We developed the contents of the video through a series of three pilot studies conducted with 16 management information systems (MIS) students in an introductory information security course. The participants in the pilot studies included a mix of 50% American and 50% International students of which only three had prior working knowledge of password managers.

To develop the fear appeal message, we followed the guidelines of Witte et al. (2001) and Ruiter et al. (2014) in building our message about the dangers of poor password management and a recommended response. For instance, Witte et al. (2001) state that successful fear appeals must include two components, which our threat (fear appeal) message has both. First, the fear appeal must have a threat component that articulates the magnitude of the threat and the real possibility that the danger associated with the threat can occur to the participant (on a personal level). Second, the fear appeal must include a recommended response that communicates that the prescriptive solution works, is within the capability of the recipient to implement, and addresses common barriers from performing the designated response. After watching the fear appeal video, we captured self-reported perceptions of the PMT constructs including each subject's self-reported protection motivation to adopt the LastPass password manager voluntarily. At this stage of our study, we also measured each individual's level of uncertainty avoidance (along with all of the other Hofstede dimensions).

One week after completing the first part of the study, we captured the actual security behaviors of the participants (i.e., did they or did they not adopt the LastPass password manager). In order to alleviate the potential problems associated with a self-reported actual use measure (i.e., subjects not wanting to admit to the researchers that they did not adopt the password manager), we asked several questions that could be answered only by using the "Security Challenge" tool built in LastPass. If the subjects did not actually adopt the tool, then the participants would not be able to answer these questions. These items included the relative strength of their master password, total security score for all their accounts, and total number of accounts in their password manager application after initial use.

4.1. *Participants*

We used a sample of 227 undergraduate business students from a private US university with a sizable international population. In return for participation, the subjects earned course extra credit (between 1 and 2% of their overall course grade depending on the instructor). Our sample was composed of 62% North American, 22% Asian, 10% European, and 6% Middle Eastern. In our paper, we are generalizing to the theory of Lee and Baskerville (2003). Therefore, this sample provided adequate variance along the uncertainty avoidance cultural dimension (and the PMT constructs) to test our proposed relationships empirically. Additionally, this population typically has a large number of password protected online accounts so they can benefit from the voluntary use of password managers, but this age demographic has very low adoption rates of password managers (Drennan et al., 2006).

4.2. *Constructs and measures*

We adapted measurement items for all of our constructs from pre-validated (reflective) scales taken from previous PMT ISP-compliance and national culture research. Table 1 displays the specific items, citations, and additional details. We measured all items reflectively using 7-point Likert scales ranging from (1) strongly disagree to (7) strongly agree.

Cultural theorists continue to debate the proper way to measure Hofstede's national culture dimensions (Kirkman et al., 2006; McCoy et al., 2005; Sivakumar and Nakata, 2001). Some scholars argue that Hofstede dimensions should be measured at the individual level of analysis (Brockner, 2005; Srite and Karahanna, 2006), whereas other scholars are steadfastly opposed to measuring culture at the individual level (Bochner and Hesketh, 1994; Hofstede, 2001; Palich et al., 1995). Part of the contention rests on the definition of Hofstede dimensions. For instance, if uncertainty avoidance is defined as a property of the culture (i.e., Greece is a high uncertainty avoidance culture), then measuring uncertainty avoidance at the individual level may be misleading. However, if uncertainty avoidance is defined as an individual's perception of ambiguity and uncertainty, then measuring uncertainty avoidance at the individual level is justified.

Table 1 – Construct definitions and measurement items.

Construct	Definition and Item Source(s)	Survey Question/Measurement Item	Item	Factor Load	Mean	Std Dev
Protection motivation intention	Self-reported intention to perform a security-related behavior. Items adapted from Ajzen (1991), Boss et al. (2015).	I intend to use a password manager in the next week.	PMI1	0.927	4.11	1.538
		I predict I will use a password manager in the next week.	PMI2	0.983	4.05	1.536
		I plan to use a password manager in the next week.	PMI3	0.907	4.16	1.524
Perceived threat vulnerability	"How personally susceptible an individual feels to the communicated threat" (Milne et al., 2000, p. 108). Items adapted from Boss et al. (2015)	My online account passwords are at risk of being stolen and abused by cyber-criminals	PVUL1	0.804	4.92	1.302
		It is likely that my online account passwords will be stolen and abused by cyber-criminals.	PVUL2	0.745	4.07	1.343
		It is possible that my online account passwords will be stolen and abused by cyber-criminals.	PVUL3	0.679	5.11	1.364
Perceived threat severity	"How serious the individual believes that the threat would be" to him- or herself (Milne et al., 2000, p. 108). Items adapted from Boss et al. (2015).	If my online account passwords were stolen and abused by cyber-criminals, it would be severe.	TSEV1	0.983	5.65	1.276
		If my online account passwords were stolen and abused by cyber-criminals, it would be serious.	TSEV2	0.900	6.04	1.03
		If my online account passwords were stolen and abused by cyber-criminals, it would be significant.	TSEV3	0.811	5.95	1.176
Self-efficacy	"The perceived ability of the person to actually carry out the adaptive [coping] response" (Floyd et al., 2000, p. 411; Rogers, 1983). Items adapted from Boss et al. (2015).	Password manager software is easy to use.	SE1	0.806	5.29	1.091
		Password manager software is convenient to use.	SE2	0.83	5.13	1.185
		I am able to use password software without much effort.	SE3	0.81	5.1	1.197
Response efficacy	"The belief that the adaptive [coping] response will work, that taking the protective action will be effective in protecting the self or others" (Floyd et al., 2000, p. 411; Rogers, 1983). Items adapted from Boss et al. (2015).	Password manager applications work to protect my online account passwords from being stolen and abused by cyber-criminals.	REFF1	0.876	5.81	1.009
		Password manager applications are an effective solution to protect my online account passwords from being stolen and abused by cyber-criminals.	REFF2	0.907	5.76	0.981
Uncertainty avoidance	The self-reported degree to which one accepts ambiguous or uncertain situations. Items adapted from Hofstede et al. (2010); Yoo et al., (2011). Items adapted from Boss et al. (2015).	Rules and regulations are important because they inform employees what the organization expects of them.	UA1	0.89	5.73	0.997
		Standard operating procedures are helpful to employees on the job.	UA2	0.923	5.69	0.961
		Order and structure are very important in a work environment.	UA3	0.648	5.7	1.025
Fear	A negatively valenced emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a general negative mood, and it manifests itself emotionally, cognitively, and physically (Leventhal, 1970; McIntosh et al., 1997; Osman et al., 1994; Witte, 1992, 1998; Witte et al., 1996). Items adapted from Boss et al. (2015).	I am worried about the prospect of having my online account passwords stolen and abused by cybercriminals.	FEAR1	0.764	4.93	1.427
		I am frightened about the prospect of having my online account passwords stolen and abused by cybercriminals.	FEAR2	0.864	4.85	1.455
		I am anxious about the prospect of having my online account passwords stolen and abused by cybercriminals.	FEAR3	0.92	4.48	1.644
Maladaptive rewards	The general rewards (intrinsic and extrinsic) of not protecting oneself, contrary to the fear appeal (Floyd et al.,2000; Rogers & Prentice-Dunn, 1997). Items adapted from Boss et al. (2015).	Using a password manager would interfere with other programs on my computer.	MAL1	0.847	4.37	1.455
		Using a password manager would limit the functionality of computer.	MAL2	0.922	3.5	1.428
		Using a password manager would interfere with other programs on my computer.	MAL3	0.903	3.88	1.479
Response costs	"Any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response" (Floyd et al., 2000) Items adapted from Boss et al. (2015).	Using a password manager application on my computer would require considerable investment of effort other than time.	COST1	0.815	3.65	1.466
		Using a password manager application would be time consuming.	COST2	0.818	3.85	1.541

Srite and Karahanna (2006) argue that it is necessary to measure the Hofstede (and all cultural dimensions) dimensions at the individual-level, because individuals interact with many different cultures from all around the world throughout their lives. The multi-cultural nature of today's global citizens may change their individual perceptions related to the Hofstede dimensions in relation to the Hofstede scores from their national culture of origin. Measuring at the individual-level also avoids the ecological fallacy of deducing individual-level characteristics based on the characteristics of the group (or one of the several groups) to which an individual belongs. Therefore, we follow Srite and Karahanna (2006) and many others by measuring the Hofstede dimensions at the individual level in our study.[1]

4.3. *Data analysis technique*

We used covariance-based structural equation modeling (CBSEM) to evaluate our theorized relationships in the PMT. CBSEM is an appropriate analysis method when testing explanatory relationships between latent constructs of a theoretically derived, *a priori* model (Raykov and Marcoulides, 2006), which is the case for our proposed research model. Prior to conducting CBSEM analyses, we successfully screened our data for issues that may jeopardize the results, such as outliers, multicollinearity, and non-normality (Byrne, 2001).

We followed the guidance of Gefen et al. (2011) and Podsakoff et al. (2003) to assess potential common method bias. First, we used the security challenge to objectively determine actual use, which mitigates this problem for actual usage but not for protection motivations. Second, we used survey best practices to minimize the possible impact of common method bias (Dillman et al., 2014). For instance, we made study participation voluntary and anonymous. We also paid careful attention to the wording on the instructions whereby we specifically stated that there were no right or wrong answers so respondents would have a greater likelihood of answering honestly. Third, we conducted a post-hoc confirmatory factor analysis to assess the potential presence of common method bias. To do this post-hoc analysis, we entered all model variables into an exploratory factor analysis model using principal-component analysis with varimax rotation and un-rotated, principal-component analysis. This post-hoc confirmatory factor analysis revealed no major issues. While the results of the above steps and statistical analyses do not completely negate the possibility of common method variance, they do suggest that it is not a major concern in these data.

5. Results

CBSEM analysis consists of two parts: (1) a confirmatory factor analysis (CFA) stage and (2) the structural model analysis (also known as path analysis) stage (Heck, 1998).

5.1. *CFA and instrument validity*

The CFA stage assesses the quality and validity of the construct measures. We performed this analysis on the entire set of measurement items for all latent constructs simultaneously with each observed variable restricted to load on its *a priori* factor. Table 1 displays the measurement item loadings on their respective constructs. For our sample, all factor loadings are in the range of 0.648–0.983. While the recommended threshold for item loadings is 0.7, individual item loadings between .40 and .70 are acceptable for inclusion so long as composite reliabilities are above .70 (which they are for all of our constructs) (Chin, 1998). We also examined the average variance extracted (AVE) to ensure individual item reliability and convergent validity. In our data, all of the AVE values were greater than the minimum recommended threshold of 0.50, which further indicates that the items satisfied the convergent validity requirements, as shown in Table 2.

To assess the discriminant validity of the latent constructs in our research model, we examined the AVE, maximum shared squared variance (MSV), and average shared squared variance (ASV) metrics (see Table 2). In our data, the MSV and ASV were both less than the AVE, which is evidence of discriminant validity because the construct items load more on their respective latent variables than on other constructs (Hair et al., 2010). Based upon the criteria set forth in Jarvis et al. (2003) and Petter et al. (2007), all of the construct measures met the requirements to be considered as reflective indicators of their respective latent constructs. Finally, the model fit for the CFA analysis (which include all latent constructs) was satisfactory ($\chi 2/\mathrm{df} = 1.532$; CFI = 0.963; SRMR = .0460).

5.2. *Structural model analysis*

Following establishment of the measurement model in the CFA stage, we fit the data to the *a priori* research models. As previously mentioned, there are many different variations of the PMT that have been published in the behavioral information security literature. As such, we evaluate our three uncertainty avoidance hypotheses in relation to the core PMT following Warkentin et al. (2016) and the full PMT following Boss et al. (2015) and Posey et al. (2015).

In both cases, we assessed model fit using multiple criteria such as chi-square, degrees of freedom, and normed chi-square ($\chi 2/\mathrm{df}$) (Heck, 1998; Kline, 2011; Raykov and Marcoulides, 2006). To further account for the potential impact of even mild deviations from perfectly normal data distributions on the $\chi 2$ calculations, we conducted Bollen and Stine (1992) bootstrapping to calculate model fit p-values, which were all above the common 0.05 threshold for the core and full PMT structural models. For both sets of models, we also used one goodness-of-fit (comparative fit index (CFI)) and one badness-of-fit (standardized root mean square residual (SRMR)) metric to further assess overall model fit (Kline, 2011). For both sets of models (core and full PMT models), the CFI values were above the 0.90 (Marsh et al., 2004) and 0.95 recommended thresholds and the SRMR badness-of-fit metrics were below the common threshold of 0.08 (Hu and Bentler, 1999). All of these metrics indicate good overall model fit for all of the core and full PMT models.

[1] We also compared the individual level values with Hofstede's reported country scores (where available). In our sample, none of the individual level values were materially different from Hofstede's published values.

Table 2 – Confirmatory factor analysis results for full and core PMT Models.

Construct	CR	AVE	MSV	ASV	PMI	PVUL	TSEV	FEAR	MAL	COST	REFF	SEFF	UA
PMI	0.958	0.883	0.203	0.095	0.940								
PVUL	0.788	0.554	0.187	0.068	0.219	0.744							
TSEV	0.928	0.811	0.120	0.058	0.200	0.269	0.901						
FEAR	0.924	0.753	0.141	0.060	0.318	0.375	0.335	0.867					
MAL	0.722	0.794	0.412	0.089	–0.317	0.041	–0.077	0.115	0.891				
COST	0.800	0.667	0.412	0.112	–0.392	0.034	–0.148	–0.002	0.642	0.817			
REFF	0.880	0.712	0.228	0.108	0.337	0.433	0.347	0.198	–0.149	–0.160	0.844		
SEFF	0.856	0.665	0.263	0.129	0.451	0.299	0.214	0.263	–0.338	–0.513	0.478	0.815	
UA	0.866	0.688	0.125	0.031	–0.031	0.051	0.214	0.025	–0.197	–0.127	0.353	0.148	0.829

Construct	CR	AVE	MSV	ASV	SNORM	BINT	LTO	ATT	SEFF
SNORM	0.829	0.621	0.365	0.140	0.788				
BINT	0.958	0.883	0.365	0.201	0.604	0.940			
LTO	0.794	0.567	0.057	0.030	–0.121	0.036	0.753		
ATT	0.905	0.762	0.237	0.144	0.343	0.487	0.239	0.873	
SEFF	0.856	0.664	0.203	0.119	0.249	0.450	0.219	0.406	0.815

CR = composite reliability, AVE = average variance extracted, MSV = maximum shared squared variance, ASV = shared squared variance, PMI = protection motivation intention, SEFF = self-efficacy, PVUL = perceived vulnerability, TSEV = threat severity, MAL = maladaptive rewards, COST = response costs, REFF = response efficacy, UA = uncertainty avoidance, BINT = behavioral intent, ATT = Attitude, LTO = long term orientation.

5.2.1. *Structural model analysis for core PMT*

Fig. 4 graphically displays our three hypotheses in relation to the core PMT. Table 3 displays the model fit results and the path coefficients for the four models that we used to empirically evaluate our hypotheses. Model 1 is the core PMT only model. The path coefficients have the proper sign but the only path coefficient that is statistically significant is self-efficacy. Model 2 contains the core PMT constructs along with uncertainty avoidance as a direct antecedent to protection motivation. In this model, response efficacy became significant, self-efficacy remained highly significant as well, and the main effect of uncertainty avoidance was a significant predictor of protection motivation intentions. However, the direction of the uncertainty avoidance main effect was opposite from what we predicted in H1. Those individuals who reported higher levels of uncertainty avoidance (i.e., uncomfortable with uncertainty) had lower (not higher) protection motivation. However, uncertainty avoidance was part of a statistically significant higher order interaction effect in Models 3 and 4.

Model 3 contained the interaction effect of uncertainty avoidance and perceived threat vulnerabilities. Model 4 included the interaction effect of uncertainty avoidance and perceived threat severity. Model fit for both Models 3 and 4 were satisfactory (Model 3: $\chi2$ / df = 1.451, CFI = 0.979, and SRMR = .0432; Model 4: $\chi2$ / df = 1.441, CFI = 0.98, and SRMR = .0434) and each had more explained variance relative to the main effects only model (Model 2). Fig. 5 displays both interaction effects.

Model 3 showed that the effect of perceived vulnerability on protection motivations is positive for individuals who report an above average level of uncertainty avoidance, but negative for individuals who report an average or below average level of uncertainty avoidance. The differential effect of uncertainty avoidance on perceived threat vulnerabilities was greater for those individuals reporting a below average level of uncertainty avoidance relative to an above average level of uncertainty avoidance. Interestingly, Model 3 revealed the highest protection motivations came for individuals who had a below average perceived threat vulnerability. Therefore, Model

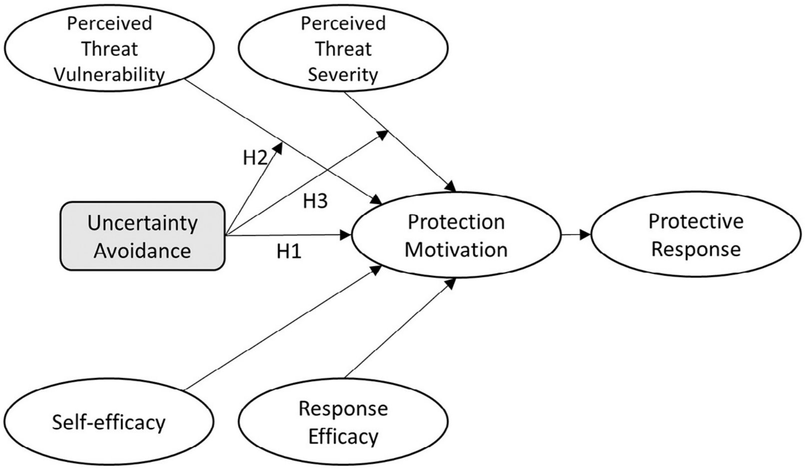

Fig. 4 – Hypotheses using core PMT.

Table 3 – Structural model analysis results (Core PMT).

SEM Model Fit Results	1: Core PMT Only	2: Core PMT with UA	3: Core PMT UAxPVUL	4: Core PMT UAxTSEV
χ2 / df	1.528	1.49	1.451	1.441
χ2	120.697	177.356	190.038	188.773
df	79	119	131	131
Comparitive Fit Index (CFI)	0.983	0.979	0.979	0.98
Standardized Root Mean Residual (SRMR)	0.0439	0.0444	0.0432	0.0434
Squared Multiple Correlation (SMC)	0.228	0.253	0.268	0.274
SEM Structual Path Results				
PVUL → BINT	0.028	0.003	(–)0.011	0.009
TSEV → BINT	0.076	0.094	0.096	0.085
REFF → BINT	0.124	*0.190	*0.209	*0.202
SEFF → BINT	**0.365	**0.363	**0.359	**0.357
UA → BINT		*(–)0.172	*(–)0.171	*(–)0.151
UA x PVUL Interaction → BINT			*0.124	
UA x TSEV Interaction → BINT				*0.147

Note: $^{*}p < 0.05$, $^{**}p < 0.001$ BINT = behavioral intent, SEFF = self-efficacy, PVUL = Perceived Vulnerability, TSEV = Threat Severity, REFF = Response Efficacy, UA = Uncertainty Avoidance.

3 supports our H2 qualifying relationship, albeit in a slightly different direction than what we predicted.

Model 4 showed that the effect of perceived threat severity on protection motivations is positive for those individuals who report an above average or average level of uncertainty avoidance, but slightly negative for those individuals who report a below average level of uncertainty avoidance. The differential effect of uncertainty avoidance on perceived threat severity was greater for those individuals reporting an above average level of uncertainty avoidance relative to a below average level of uncertainty avoidance. Similar to Model 3, the highest protection motivation came for individuals who reported a below average level of uncertainty avoidance and a low perceived threat severity. Therefore, Model 4 supports our H3 qualifying relationship, albeit in a slightly different direction than what we predicted.

5.2.2. *Structural model analysis for the full PMT*

Fig. 6 graphically displays our three hypotheses in relation to the full PMT following Boss et al. (2015) and Posey et al. (2015). Table 4 displays the model fit results and the path coefficients for the four models that we used to evaluate our hypotheses empirically in connection to the full PMT. The results when using the full PMT are the same in terms of the sign and statistical significance of each of the hypothesized variables except the interaction effect of perceived threat vulnerability and uncertainty avoidance in Model 7 is only significant at the 0.1 level.

5.2.3. *Post-hoc descriptive data analysis of actual adoption rates*

We performed a post-hoc descriptive data analysis of actual adoption rates of the recommended security behavior (use of the password manager LastPass), which provides additional support for the impact of uncertainty avoidance (UA), protection motivation intentions (PMI), and actual use of password managers by our study participants. Table 5 displays the actual adoption rates for our sample broken down by the main constructs in the proposed theoretical model (PMI, UA, perceived threat vulnerability (PVUL), and perceived threat severity (TSEV)) where "low" indicates participants with at and below-average scores for the respective variable and "high" is above average. Table 5 shows that those individuals with low PMI have a statistically significantly lower actual security behavior adoption

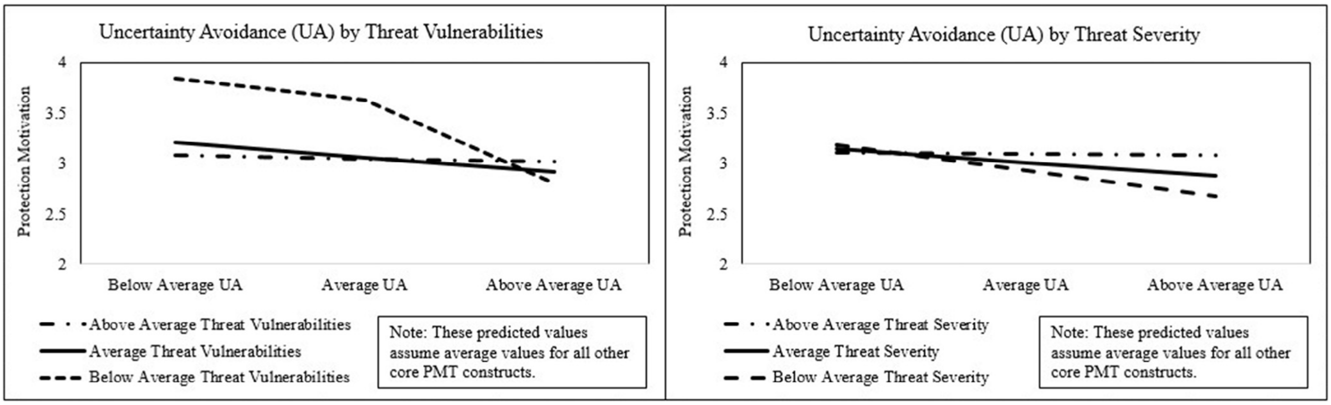

Fig. 5 – Interaction effects in Models 3 and 4.

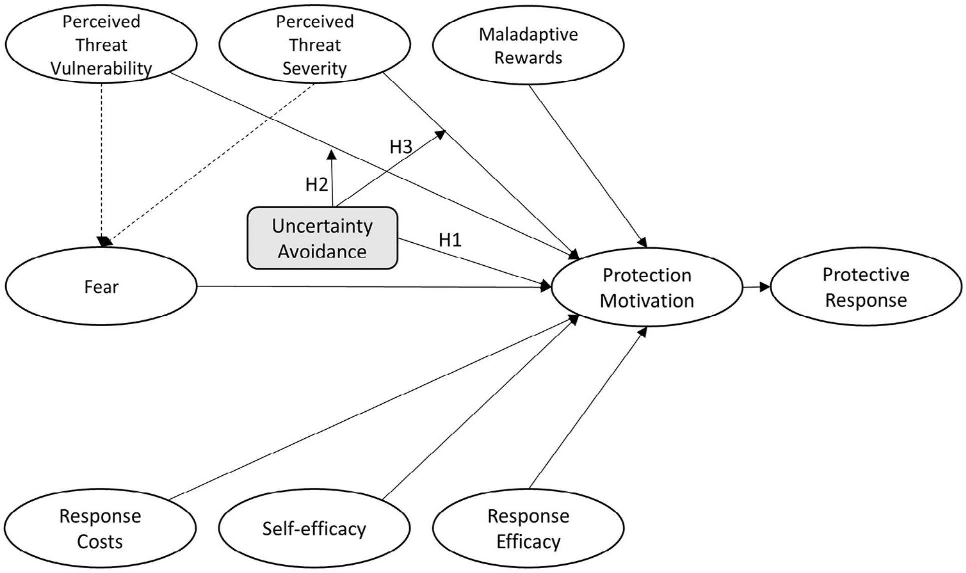

Fig. 6 – Hypotheses using full PMT.

rate (Pearson Chi-square F = 10.548, p = 0.001) than those individuals with high PMI. While the actual security behavior adoption rate for high PMI participants is still well below 100%, this data provides support to the assumption that higher intentions generally lead to higher actual behavior rates (Ajzen, 1991).

Our research model predicts the direct and qualifying relationships between UA on TSEV, PVUL, and protection motivation intention (PMI). We make no predictions concerning actual behaviors. Table 5 shows the actual adoption rates for participants with above and below average scores for these constructs. As expected, none of the variables had a significant direct contribution to actual security behaviors as their impact on actual behavior was evident through the increase or decrease in PMI. However, Table 5 does show actual adoption rates were in the same direction as the PMI dependent variable. For example, actual voluntary adoption rates were higher for participants with lower UA, lower TSEV, and higher PVUL scores.

Table 6 provides a deeper look into the relationship among UA, PMI and actual security behavior. Participants with below average PMI saw their security behavior intentions and actual adoption behaviors decrease with increasing UA, keeping with the general results seen in the earlier analysis of the theoretical model. However, for those with above average PMI, we saw the opposite effect whereby both PMI and actual voluntary

Table 4 – Structural model analysis results (Full PMT).

SEM Model Fit Results	5: Full PMT Only	6: Full PMT with UA	7: Full PMT UAxPVUL	8: Full PMT UAxTSEV
χ2 / df	1.569	1.484	1.461	1.454
χ2	318.602	393.194	413.515	411.578
df	203	265	283	283
Comparitive Fit Index (CFI)	0.967	0.967	0.967	0.967
Standardized Root Mean Residual (SRMR)	0.486	0.491	0.481	0.486
BINT Squared Multiple Correlation (SMC)	0.315	0.341	0.348	0.351
Fear Squared Multiple Correlation (SMC)	0.195	0.197	0.199	0.197
SEM Structual Path Results				
PVUL → Fear	0.303***	0.304***	0.307***	0.303***
TSEV → Fear	0.250***	0.253***	0.252***	0.253***
PVUL → BINT	0.034	0.014	0.003	0.018
TSEV → BINT	(–)0.009	0.016	0.017	0.01
Fear → BINT	0.238***	0.233***	0.227***	0.223**
MAL → BINT	(–)0.073	(–)0.099	(–)0.087	(–)0.076
REFF → BINT	0.155 *	0.222**	0.236**	0.232**
SEFF → BINT	0.171 (p = 0.0742)	0.163 (p = 0.084)	0.167 (p = 076)	0.166 (p = 0.075)
COST → BINT	(–)0.219	(–)0.210	(–)0.211	(–)0.218
UA → BINT		(–)0.181**	(–)0.179**	(–)0.162*
UA ×PVUL Interaction → BINT			0.097 (p = 0.9)	
UA × TSEV Interaction → BINT				0.115*

Note: $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$ BINT = behavioral intent, SEFF = self-efficacy, PVUL = perceived vulnerability, TSEV = threat severity, REFF = response efficacy, UA = uncertainty avoidance, MAL = maladaptive rewards, COST = response cost.

Table 5 – Actual security behavior adoption rates.

	UA	TSEV	PVUL	PMI	
# of participants	101	81	110	122	Below
# actual behavior	17	15	13	9	Average
% actual behavior	16.80%	18.50%	11.80%	7.40%	
# of participants	126	146	117	105	Above
# actual behavior	18	20	22	25	Average
% actual behavior	14.20%	13.70%	18.80%	23.80%	

PMI = protection motivation intention, TSEV = perceived threat severity, PVUL = perceived vulnerability, UA = uncertainty avoidance, Actual Behavior means adopted use of a password manager as a result of participating in this study.

Table 6 – Uncertainty avoidance, protection motivation, and actual behavior.

	Low UA	High UA	
# of participants	55	67	Low PMI
Mean PMI	3.03	2.95	
% actual behavior	10.90%	6%	
# of participants	46	59	High PMI
Mean PMI	5.39	5.429	
% actual behavior	21.70%	23.70%	

PMI = protection motivation intention, TSEV = perceived threat severity, UA = uncertainty avoidance, Actual Behavior means adopted use of a password manager as a result of participating in this study.

adoption rates increased with higher UA. There is not a statistically significant difference between the adoption rates for the different UA and PMI low/high categories, but the trend of the results indicates that it is possible that the effect of UA on PMI only translates over to actual behavior when protection motivation intentions are below average. For participants with above average PMI, the relationship between intent and actual behavior is much stronger, which supersedes the effect of UA.

5.2.4. *Impact of the other Hofstede dimensions*

Although we were only theoretically interested in the impact of UA on PMI and actual behaviors in this paper, we tested the potential influence of the other Hofstede dimensions in the PMT. In some samples, Hofstede's long-term orientation dimension and uncertainty avoidance dimension of national culture are highly correlated, because how an individual perceives uncertainty might influence whether that individual is more long-term or short-term oriented. In other words, there is a varying amount of risk taking associated with being long-term or short-term oriented (Fang, 2003). We did not have excessively high correlations between these two constructs in our data (measured at the individual level), but we did repeat all of our analyses with Hofstede's long-term orientation cultural dimension instead of UA. In those models, both the main effect and the qualifying effect of long-term orientation were not statistically significant in either the core or the full PMT models.

Given our threat context (poor password management threat and the password manager coping mechanism) and the voluntary nature of the information security related behavior, none of the other Hofstede dimensions make conceptual sense in relation to the PMT but we tested them in an exploratory manner anyways. We repeated all of our analyses using the core and full PMT models with each of the other four Hofstede dimensions instead of UA. None of the other remaining four Hofstede dimensions had a direct or qualifying effect on PMI. UA was the only one of Hofstede dimensions that had either a direct or a qualifying effect on PMI in our sample.

6. Discussion and conclusion

The primary theoretical contribution of our study was to include national culture (specifically the uncertainty avoidance dimension) in the PMT. We theoretically and empirically investigated the main and qualifying effect of the uncertainty avoidance dimension of national culture in the context of the PMT. We hypothesized that the effect would be positive (i.e., individuals with a higher discomfort with uncertainty would be more motivated to adopt a voluntary information security control), but we found the effect to be negative. We believe that this is the case because there are two elements of uncertainty at play in the context of password managers. There is the uncertainty pertaining to the technology (i.e., LastPass password manager) and the uncertainty associated with the threat (i.e., compromised password). The uncertainty avoidance that appeared to be playing out in our study was the uncertainty associated with storing all of their passwords in a single location. Therefore, the "tried and tested" approach was not the mature password manager application as we theorized, but instead was the manual process that our subjects were currently using.

In our follow-up conversations and our study debriefing, our participants indicated that they had the mindset that what they were currently doing (manual process using poor password management practices) was working. For the most part, they were comfortable with their current processes even though those processes may have resulted in suboptimal password management practices. From this perspective, the negative relationship between uncertainty avoidance and protection motivation might make sense. Future research may want to compare the two different elements of uncertainty associated with voluntary information security controls in a more explicit manner. Investigating the uncertainty between the threat appraisal and the coping mechanism would further tease out the effect of uncertainty avoidance in the PMT.

We also found that the differential effect of uncertainty avoidance on perceived threat vulnerabilities was greater for those individuals reporting a below average level of uncertainty avoidance relative to an above average level of uncertainty avoidance, but we found the opposite qualifying effect on perceived threat severity. This difference may be the case because a high perceived threat severity activates the uncertainty avoidance in connection with the threat whereas the high perceived vulnerability of the college students in our sample did not. For example, the perceived vulnerability associated with a cracked password for a college student is still probably low relative to a 40- or 50-year-old professional who might have much more to lose (in terms of a bank account getting broken into or having her professional reputation tarnished). Nevertheless, the implication of this finding is that different levels of uncertainty avoidance do influence both the core and full PMT models. Therefore, future PMT research should, at a minimum, consider the cross-national differences when researching protection motivation intentions and actual behaviors.

The post-hoc descriptive analysis of actual adoption rates also revealed some interesting (possibly counter-intuitive) results. Those participants who reported a below average protection motivation and a below average level of uncertainty avoidance had a greater likelihood of actually adopting the password manager relative to those who had a similarly low protection motivation but an above average level of uncertainty. We found the opposite relationship for those who reported a high level of uncertainty avoidance and high protection motivations. We suggest that this means that having high protection motivation intentions activate the uncertainty avoidance cultural dimension associated with the threat and the coping mechanism (i.e., adopting the password manager software). However, low protection motivations does not activate this particular cross-cultural difference dimension.

We investigated a single theoretically relevant cross-cultural construct in our paper. However, in a different threat context with a different theoretical framework, different cultural dimensions may be more relevant. For example, for a socially interactive threat such as tailgating it would be reasonable to predict that power distance would have a direct, indirect, or qualifying impact on protection motivations, because there is a status dynamic associated with the tailgating threat and control (Aurigemma and Mattson, 2017). Therefore, a fruitful area of future research can investigate other threat contexts and other national cultural dimensions in the context of the core and full PMT models.

Although we investigated password manager applications in our paper, we make no claims that these applications are the only solution to solving the problem of poor password management. For instance, federated systems such as Facebook, Yahoo, or Google where a user logs into one system and is granted access to multiple other systems also aim to solve the problems that individuals have regarding poor password management. There is a different element of uncertainty associated with federated systems, which may change our proposed relationships. For example, privacy issues might be a bigger concern with a federated system such as Google, which may intensify the uncertainty associated with the technology and maximize the certainty associated with not changing an individual's current manual password management process. Therefore, an interesting future study would be to test our research model using a federated system.

Like all research, our study has limitations. First, we only investigated the effects in connection with PMT. As we previously mentioned, there is no consensus among behavioral information security researchers as to which theoretical approach is best. Therefore, future research can investigate the effect of uncertainty avoidance (and other cultural dimensions) in other models such as the TPB, rational choice, or psychological capital. Second, we had significant variance of uncertainty avoidance of our survey participants to test our proposed research model, but our sample did not include any participants from the highest and the lowest extreme uncertainty avoidance cultures. Extreme cultures such as Greece (high) and Singapore (low) might strengthen or weaken our reported path coefficients. Therefore, future research might focus on the extreme cultures to further empirically test our theorized relationships. Finally, we only had a single fear appeal message that all of the study participants watched. It is possible that different cultures respond to fear appeals differently. As such, different fear appeals might influence our proposed qualifying effects (either strengthen or weaken our reported results). An interesting future study might be to conduct a random experiment with multiple fear appeals with a culturally diverse sample of participants along a single (or multiple) cultural dimensions.

As with most other cross-cultural research, the main practical contribution of our study is that it is important for information security managers to know the composition and behavioral orientations of the people receiving security-related training in order to maximize their effectiveness. For instance, in the university where we collected the data for our study, basic security awareness training and documentation are designed in a one-size-fits-all paradigm where the same message is expected to engender positive behavioral change for all information system users, regardless of age, gender, education level, IT experience, or national culture. Karjalainen et al. (2013) cogently stated that "while information security behaviors are learned, different paradigms of learning are effective in different cultures; i.e., different cultures require different IS security interventions." (p. 1). Particularly in culturally diverse organizations, ignoring the effect of cultural dimensions such as uncertainty avoidance, and possibly other cultural characteristics, can have a deleterious impact on the overall organizational information security posture.

REFERENCES

Ajzen I. The theory of planned behavior. Organ Behav Hum Decis Process 1991;50(2):179–211.

Albrechtsen E. A qualitative study of users' view on information security. Comput Secur 2007;26(1):276–89.

Aurigemma S. A composite framework for behavioral compliance with information security policies. J Org End User Comput 2013;25(3):32–51.

Aurigemma S, Mattson T. Privilege of procedure: evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. Comput Secur 2017;66(1):218–34.

Bochner S, Hesketh B. Power distance, individualism/collectivism, and job-related attitudes in a culturally diverse work group. J Cross Cult Psychol 1994;25(2):233–57.

Bollen KA, Stine RA. Bootstrapping goodness-of-fit measures in structural equation models. Sociol Methods Res 1992;21(2):205–29.

Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly 2015;39(4):1.

Brockner J. Unpacking country effects: on the need to operationalize the psychological determinants of cross-national differences. In: Staw BM, Sutton RL, editors. Research in organizational behavior. Greenwich, CT: JAI Press; 2005. p. 335–69.

Byrne BM. Structural equation modeling with AMOS, EQS, and LISREL: comparative approaches to testing for the factorial validity of a measuring instrument. Int J Test 2001;1(1):55–86.

Cardon PW, Marshall BA. National culture and technology acceptance: the impact of uncertainty avoidance. Issues Inf Syst 2008;9(2):103–10.

Chen R, Wang J, Herath T, Rao HR. An examination of an e-authentication service as an intervention in e-mail risk perception. J Inf Priv Secur 2017;1(13):2–16.

Chen Y, Zahedi FM. Individual's internet security perceptions and behaviors: polycontextual contrasts between the united states and china. MIS Quarterly 2016;40(1):205–22.

Chin WW. Commentary: issues and opinion on structural equation modeling. MIS Quarterly 1998;22(1):vii–xvi.

Choong Y-Y, Theofanos M. What 4,500+ people can tell you–employees' attitudes toward organizational password policy do matter Human Aspects of Information Security, Privacy, and Trust. Springer; 2015. p. 299–310.

Crossler R, Belanger F. An extended perspective on individual security behaviors: protection motivation theory and a Unified Security Practices (USP) instrument. ACM SIGMIS Database 2014;45(4):51–71.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur 2013;32(February):90–101.

Crossler RE, Long JH, Loraas TM, Trinkle BS. Understanding compliance with bring your own device policies utilizing protection motivation theory: bridging the intention-behavior gap. J Inf Syst 2014;28(1):209–26.

CSID. Consumer survey: password habits – a study of password habits among American consumers; 2012. Retrieved from: https://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf.

Daily B, Whatley A, Ash SR, Steiner RL. The effects of a group decision support system on culturally diverse and culturally homogeneous group decision making. Inf Manag 1996;30(6):281–9.

Dillman DA, Smyth JD, Christian LM. Internet, phone, mail, and mixed-mode surveys: the tailored design method. Hoboken, New Jersey: John Wiley & Sons, Inc; 2014.

Dinev T, Goo J, Hu Q, Nam K. User behaviour towards protective information technologies: the role of national cultural differences. Inf Syst J 2009;19(4):391–412.

Dols T, Silvius A. Exploring the influence of national cultures on non-compliance behavior. Commun IIMA 2010;10(3).

Drennan J, Sullivan GM, Previte J. Privacy, risk perception, and expert online behavior: an exploratory study of household end users. J Org End User Comput 2006;18(1):1–22.

Fang T. A critique of Hofstede's fifth national culture dimension. Int J Cross Cult Manag 2003;3(3):347–68.

Florencio D, Herley C. A large-scale study of web password habits; 2007. Paper presented at the Proceedings of the 16th international conference on World Wide Web.

Floyd DL, Prentice-Dunn S, Rogers RW. A meta-analysis of research on protection motivation theory. J Appl Soc Psychol 2000;30(2):407–29.

Garfield MJ, Watson RT. Differences in national information infrastructures: the reflection of national cultures. J Strategic Inf Syst 1997;6(4):313–37.

Gefen D, Straub DW, Rigdon EE. An update and extension to SEM guidelines for admnistrative and social science research. MIS Quarterly 2011;35(2):iii–xiv.

Hair JF, Black WC, Babin BJ, Anderson RE. Multivariate data analysis: a global perspective. Upper Saddle River, NJ: Pearson; 2010.

Hall ET. Beyond culture. New York: Doubleday; 1976.

Hasan H, Ditsa G. The impact of culture on the adoption of IT: An interpretive study. J Glob Inf Manag (JGIM) 1999;7(1):5–15.

Heck RH. Factor analysis: exploratory and confirmatory approaches. In: Marcoulides G, editor. Modern methods for business research. Mahwah, NJ: Erlbaum; 1998. p. 177–215.

Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organizations. Eur J Inf Syst 2009;18(2):106–25.

Hermeking M. Culture and internet consumption: contributions from cross-cultural marketing and advertising research. J Compu Mediated Commun 2005;11(1):192–216.

Hofstede G. Culture's consequences: comparing values, behaviors, institutions, and organizations across nations. Thousand Oaks, CA: Sage; 2001.

Hofstede G, Bond MH. The Confucius connection: from cultural roots to economic growth. Organ Dyn 1988;16(4):4–21.

Hofstede G, Hofstede GJ, Minkov M. Cultures and Organizations: Software of the Mind. Revised and expanded. third ed. New York, NY: McGraw-Hill; 2010.

House RJ, Hanges PJ, Javidan M, Dorfman PW, Gupta V. Culture, leadership, and organizations: the GLOBE study of *62 Societies*. Thousand Oaks, CA: Sage Publications, Inc; 2004.

Hovav A. How espoused culture influences misuse intention: a micro-institutional theory perspective; 2017. Paper presented at the Proceedings of the 50th Hawaii International Conference on System Sciences.

Hovav A, D'Arcy J. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea. Inf Manag 2012;49(2):99–110.

Hu L, Bentler PM. Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. Struct Equation Model 1999;6(1):1–55.

Humphries D. Best practices for workplace passwords; 2015. Retrieved from http://www.softwareadvice.com/security/industryview/password-workplace-report-2015/.

Huth A, Orlando M, Pesante L. Password Security, Protection, and Management; 2013. Retrieved from https://www.us-cert.gov/security-publications/password-security-protection-and-management.

Jarvis CB, Mackenzie SB, Podsakoff PM. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. J Consum Res 2003;30(2):199–218.

Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Quarterly 2010;34(3):549–66.

Johnston AC, Warkentin M, Siponen M. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Quarterly 2015;39(1):113–34.

Kankanhalli A, Tan BCY, Wei K-K, Holmes MC. Cross-cultural differences and information systems developer values. Decis Supp Syst 2004;38:183–95.

Kappos A, Rivard S. A three-perspective model of culture, information systems, and their development and use. MIS Quarterly 2008;32(3):601–34.

Karjalainen M, Siponen MT, Puhakainen P, Sarker S. One size does not fit all: different cultures require different information systems security interventions. Paper presented at the PACIS; 2013.

Keil M, Tan BCY, Wei K-K, Saarinen T, Tuunainen V, Wassenaar A. A cross-cultural study on escalation of commitment behavior in software projects. MIS Quarterly 2000;24(2):299–325.

Kirkman BL, Lowe KB, Gibson CB. A quarter century of "culture's consequences": a review of empirical research. J Int Bus Stud 2006;37(3):285–320.

Kline RB. Principles and practice of structural equation modeling. New York, NY: Guilford Press; 2011.

Kummer T-F, Recker J, Mendling J. Enhancing understandability of process models through cultural-dependent color adjustments. Decis Supp Syst 2016;87:1–12.

Lee AS, Baskerville RL. Generalizing generalizability in information systems research. Inf Syst Res 2003;14(3):221–43.

Lee D, Larose R, Rifon N. Keeping our network safe: a model of online protection behaviour. Behav Inf Technol 2008;27(5):445–54.

Leidner DE, Kayworth T. A review of culture in information systems research: toward a theory of information technology culture conflict. MIS Quarterly 2006;30(2):357–99.

Leventhal H. Findings and Theory in the Study of Fear Communications. In: Berkowitz L, editor. Advances in Experimental Social Psychology. New York: Academic Press; 1970. p. 119–86.

Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J Assoc Inf Syst 2010;11(7):394–413.

Lim KH, Leung K, Sia CL, Lee MKO. Is eCommerce boundary-less? Effects of individualism-collectivism and uncertainty avoidance on internet shopping. J Int Bus Stud 2004;35(6):545–59.

Lowry PB, Posey C, Roberts TL, Bennett RJ. Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. J Bus Ethics 2014;121(3):385–401.

Marsh HW, Hau K-T, Wen Z. In search of golden rules: comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. Struct Equation Model 2004;11(3):320–41.

McCoy S, Galletta DF, King WR. Integrating national culture into IS research: the need for current individual level measures. Commun Assoc Inf Syst 2005;15.

McCoy S, Galletta DF, King WR. Applying TAM across cultures: the need for caution. Eur J Inf Syst 2007;16(1):81–90.

McIntosh DN, Zajonc RB, Vig PS, Emerick SW. Facial Movement, Breathing, Temperature, and Affect: Implications of the Vascular Theory of Emotional Efference. Cognition & Emotion 1997;11(2):171–95.

Milne S, Sheeran P, Orbell S. Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. J Appl Soc Psychol 2000;30(1):106–43.

Ofcom. Adults' media use and attitudes (Report 2015); 2015. Retrieved from http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit-10years/2015_Adults_media_use_and_attitudes_report.pdf.

O'Reilly CA III, Chatman J, Caldwell DF. People and organizational culture: a profile comparison approach to assessing person-organization fit. Acad Manage J 1991;34(3):487–516.

Osman A, Barrious FX, Osman JR, Schneekloth R, Troutman JA. The Pain Anxiety Symptoms Scale: Psychometric Properties in a Community Sample. J Behav Med 1994;17(5):511–22.

Palich LE, Horn PW, Griffeth RW. Managing in the international context: testing cultural generality of sources of commitment to multinational enterprises. J Manag 1995;21(4):671–90.

Park H. Cultural impact on life insurance penetration: a cross-national analysis. Int J Manag 1993;10(3):342–50.

Petter S, Straub D, Rai A. Specifying formative constructs in information systems research. MIS Quarterly 2007;31(4):623–56.

Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol 2003;88(5):879–903.

Posey C, Roberts TL, Lowry PB, Bennett RJ, Courtney JF. Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Quarterly 2013;37(4):1189–210.

Posey C, Roberts TL, Lowry PB. The impact of organizational commitment on insiders' motivation to protect organizational information assets. J Manag Inf Syst 2015;32(4):179–214.

Putri FF, Hovav A. Employees compliance with BYOD security policy: insights from reactance, organizational justice, and protection motivation theory. Paper presented at the Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel; 2014.

Qiu L, Lin H, Leung AK. Cultural differences and switching of in-group sharing behavior between an American (Facebook) and a Chinese (Renren) social networking site. J Cross Cult Psychol 2013;44(1):106–21.

Raykov T, Marcoulides GA. A first course in structural equation modeling. Mahwah, NY: Lawrence Erlbaum; 2006.

Rogers RW. A protection motivation theory of fear appeals and attitude change. J Psychol 1975;91(1):93–114.

Rogers RW. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. Soc Psychophysiol 1983;153–76.

Rogers RW, Prentice-Dunn S. Protection Motivation Theory. In: Gochman DS, editor. Handbook of Health Behavior Research I: Personal and Social Determinants. New York: Plenum Press; 1997. p. 113–32.

Ruiter RAC, Kessels LTE, Peters G-JY, Kok G. Sixty years of fear appeal research: current state of the evidence. Int J Psychol 2014;49(2):63–70.

Schein EH. Organizational culture and leadership. San Francisco: Jossey-Bass; 2010.

Siponen M, Mahmood MA, Pahnila S. Employees' adherence to information security policies: an exploratory field study. Inf Manag 2014;51(2):217–24.

Sivakumar K, Nakata C. The stampede toward Hofstede's framework: avoiding the sample design pit in cross-cultural research. J Int Bus Stud 2001;32(3):555–74.

Srite M, Karahanna E. The role of espoused national cultural values in technology acceptance. MIS Quarterly 2006;30(3):679–704.

Stobert E, Biddle R. The password life cycle: user behaviour in managing passwords. Paper presented at the Symposium On Usable Privacy and Security (SOUPS 2014); 2014.

Straub DW. The effect of culture on it diffusion: e-mail and FAX in Japan and the U.S. Inf Syst Res 1994;5(1):23–47.

Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS Quarterly 1998;22(4):441–69.

Sundqvist S, Frank L, Puumalainen K. The effects of country characteristics, cultural similarity and adoption timing on the diffusion of wireless communications. J Bus Res 2005;58(1):107–10.

Triandis HC. Culture and social behavior. New York: McGraw-Hill, Inc; 1994.

Trompenaars F, Hampden-Turner C. Riding the waves of culture: understanding cultural diversity in business. London: Nicholas Brealey Publishing; 2011.

van Schaik P, Jeske D, Onibokun J, Coventry L, Jansen J, Kusev P. Risk Perceptions of cyber-security and precautionary behaviour. Comput Human Behav 2017;75(October):547–59.

Veiga JF, Floyd S, Dechant K. Towards modelling the effects of national culture on IT implementation and acceptance. J Inf Technol 2001;16(3):145–58.

Wall JD, Palvia P, Lowry PB. Control-related motivations and information security policy compliance: the role of autonomy and efficacy. J Inf Priv Secur 2013;9(4):52–79.

Warkentin M, Johnston AC, Shropshire J, Barnett WD. Continuance of protective security behavior: a longitudinal study. Decis Supp Syst 2016;92(1):25–35.

Weber EU, Hsee CK. Culture and individual judgment and decision making. App Psychol Int Rev 2000;49(1):32–61.
Witte K. Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. Commun Monogr 1992;59(4):329–49.
Witte K. Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Processing Model to Explain Fear Appeal Successes and Failures. In: Anderson PA, Guerrero LK, editors. Handbook of Communication and Emotion: Research, Theory, Application, and Contexts. San Diego, CA: Academic Press; 1998. p. 423–50.
Witte K, Cameron A, McKeon JK, Berkowitz JM. Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. J Health Commun 1996;1(4):317–42.
Witte K, Meyer G, Martell D. Effective health risk messages: a step-by-step guide. Thousand Oaks: Sage Publications; 2001.
Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput Human Behav 2008;24(6):2799–816.
Yoo B, Donthu N, Lenartowicz T. Measuring Hofstede's five dimensions of cultural values at the individual level: Development and validation of CVSCALE. Journal of International Consumer Marketing 2011;23(3–4):193–210.
Zeltser L. Password managers; 2015. Retrieved from https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201310_en.pdf.

Salvatore (Sal) Aurigemma is an Assistant Professor of Computer Information Systems in the Collins College of Business at the University of Tulsa. His research explores employee information security policy compliance, improving end-user and small business information security practices, and end-user computing focusing on business spreadsheet error detection. Prior to joining the University of Tulsa, Sal supported the U.S. Department of Defense for over 20 years on active duty and in the Navy reserves in the submarine and intelligence communities. He also has over a decade of civilian experience in the Information Technology field.

Thomas Mattson is an Assistant Professor of Management at the University of Richmond. His research focuses on social interactions in electronic networks of practice, virtual communities of practice, and other electronic social structures along with assorted issues related to information security. Prior to joining academia, Thomas worked as a technology and management consultant designing and building databases and applications for firms in the consumer packaged goods, accounting, and financial industries.