Emerald Information Management and Computer Security

Effect of Long-term Orientation on Voluntary Security Actions

Journal:	*Information and Computer Security*
Manuscript ID	ICS-07-2018-0086
Manuscript Type:	Original Article
Keywords:	Information security, Account access management, password managers, Hofstede, long term orientation, planned behavior

Effect of Long-term Orientation on Voluntary Security Actions

Abstract

Purpose of this paper: The paper aims to examine the impact an individual's long-term orientation (a cultural dimension) has on their attitude, behavioral intention, and actual voluntary security actions taken in the context of the dangers related to poor account access management.

Design/methodology/approach: The paper relied upon survey data and actual usage information from a culturally diverse sample of 227 individuals that were introduced to the specific security problem and the accepted solution of using a password manager application.

Findings: The paper provides empirical evidence that the effect of positive attitudes increased when individuals were more long-term oriented but the effect was reversed for average / negative attitudes towards the voluntary security behavior. Furthermore, participants with high long-term orientation and strong positive attitudes towards the security action actually adopted password manager applications 57% more than the average adoption rate across the sample.

Research limitations/implications: Due to the research approach (survey data), security context, and sample population, the research results may lack generalizability.

Practical implications: The findings suggest that security awareness messaging and training should account for differences in long term orientation of the target audience and integrate the distinctly different types of messages that have been shown to improve an individual's participation in voluntary security actions.

What is original/value of paper: The paper addresses previous research calls for examining possible cultural differences that impact security behaviors and is the only study that has focused on the impact of long term orientation specifically on voluntary security actions.

Keywords: Information security, account access management, password managers, Hofstede, long-term orientation, planned behavior

1. Introduction

The password remains one of the primary defense mechanisms used to protect our digital data. For a variety of reasons, however, individuals often use poor password management practices such as reusing passwords across multiple websites or using generally weak passwords (CSID, 2012; Ofcom, 2015). Furthermore, cybercriminals specifically target individual passwords in order to gain access to both personal and corporate information resources, which amplifies the detrimental impact of poor password management practices (Beardsley, Hodgman, Hart, & Geiger, 2016). In organizations, corporate IT departments often mandate the use of strong passwords and require frequent password modifications on internal systems, but individuals have accounts on many other websites (i.e., banks, personal email accounts, and social media accounts) outside the organization's control. At these other websites, individuals often do not change their relatively weak passwords for extended periods of time (if ever) (Florencio & Herley, 2007; Liu, Chen, Zang, & Liang, 2018). As a result, many individuals have a single password for multiple websites, which is highly problematic, especially if the password is relatively weak (Choong & Theofanos, 2015; Stobert & Biddle, 2014).

Dedicated password manager applications such as LastPass, Dashlane, KeePass, or 1Password exist to help resolve these types of problems. A password manager is "software for storing all your passwords in one location that is protected and accessible with one easy-to-remember master passphrase" (Huth, Orlando, & Pesante, 2013, p. 2). Both the highly reputable SANS Institute and the United States Computer Emergency Readiness Team (US-CERT) recommend the use of password manager applications (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 low adoption rates (Humphries, 2015; Liu et al., 2018). In light of this voluntary adoption decision, these low adoption rates may not be surprising because convincing individuals to perform voluntary information security actions can be a daunting challenge, especially when the action requires any amount of time, energy, and thought to implement.

One unique aspect of password manager applications relative to other security software such as anti-malware or data backup applications is the initially high setup costs associated with these applications. Depending on how many (and what types of) devices and websites that individuals have, they may have to invest a significant amount of time configuring the password manager to work correctly (Aurigemma & Mattson, 2018). This endeavor can be challenging, especially for a relatively novice or non-technical individual. Therefore, a password manager is a long-term solution to the problem of poor password management. Furthermore, the on-going use of password managers requires continuous effort to maintain as users join additional or drop out of existing password protected online communities and commercial websites, which is different from the voluntary adoption of anti-spyware or anti-virus controls (i.e., controls that run automatically in the background with minimal configuration required).

Interestingly, individuals socialized in different national cultures have varying virtues oriented towards future rewards, which is referred to as long-term orientation (LTO) (Hofstede, 2001). Certain cultures such as Sierra Leon, Ghana, and Nigeria socialize their members to have a more short-term orientation (i.e., past and present are more important than the future) whereas other cultures such as China, Hong Kong, and Taiwan socialize their members to have a more long-term orientation (i.e., future is more important than the past or present). Therefore, given the future oriented nature of password manager applications, it would be reasonable to predict that individuals socialized in different national cultures with varying time orientations would have different adoption intentions and actual adoption rates. However, this conjecture has not been theoretically or empirically investigated in the prior behavioral information security literature, specifically related to password manager adoption. Therefore, the following research question is addressed in this paper:

RQ: What is the effect of long-term orientation on behavioral intentions to adopt voluntary information security controls, specifically password manager applications?

In order to theoretically and empirically answer this research question, the theory of planned behavior (TPB) was used as the theoretical foundation. The TPB has been used extensively in the behavioral information security literature but without the inclusion of LTO in any of the traditional paths (Bulgurcu, Cavusoglu, & Benbasat, 2010; Dinev & Hu, 2007; Q. Hu, Xu, Dinev, & Ling, 2011; Safa et al., 2015; Siponen, Mahmood, & Pahnila, 2014; Wynn, Williams, Karahanna, & Madupalli, 2012). Therefore, using this theory allowed the determination of the incremental impact that LTO had above and beyond the common factors that have previously been found to impact behavioral intentions to adopt (voluntarily) a variety of information security controls. The TPB also enabled contextualizing the presented LTO hypotheses in relation to previously established relationships.

To empirically test the impact of LTO in the TPB, a culturally diverse sample of 227 individuals participated in a two part survey (i.e., one measuring intentions and one measuring actual adoption). In this sample, LTO did not have a statistically significant main effect on password manager adoption intentions but it did have a qualifying effect on an individual's attitudes towards adoption. The data show that the effect of positive attitudes on intentions to take voluntary security actions increased when individuals were more long-term oriented (relative to short-term oriented) but the effect was reversed for negative attitudes. The implication of these findings is that a one-size fits all approach to encourage voluntary information security actions (or intentions thereof) may not be the best approach, because individuals from different cultures have varying beliefs and values along many dimensions including (but not limited to) time orientation. Instead of relying upon a single set of culture-blind security messages and training for an "average" employee or individual, attention should be given to provide content in the security messaging that activates the inherent cultural biases of different individuals towards more positive attitudes and implementation of voluntary security actions.

2. Theoretical Foundations

The existing research has relied on a number of theories such as psychological capital, general deterrence theory (GDT), the theory of planned behavior (TPB), protection motivation theory (PMT), and rational choice theory to explain the variability in information security related behaviors (Aurigemma, 2013; Crossler et al., 2013). There are pros and cons associated with each one of these theoretical approaches. Therefore, under a given set of circumstances we can make a valid argument to use each one of them. Furthermore, there is no consensus among behavioral information security researchers as to which theory is the most appropriate to use for a specific situation, sample, and security-related action. For instance, the GDT may be more appropriate for mandatory information security actions whereas the TPB or PMT may be more appropriate for voluntary security actions. In this paper, the TPB is used because it is a parsimonious theory where the core paths are typically statistically significant with an average to above average amount of explained variance in a variety of information security contexts (Aurigemma & Mattson, 2017; Bulgurcu et al., 2010; Dinev & Hu, 2007; Guo, Yuan, Archer, & Connelly, 2011; Ifinedo, 2014; Siponen et al., 2014).

2.1.The Theory of Planned Behavior

The TPB assumes that individuals act rationally whereby their choices and behaviors are governed (in large part) by their behavioral intentions (Ajzen, 1991). The TPB specifically theorizes that individual actions are determined by attitudes (positive or negative state of mind), subjective norms (social pressures from relevant others), and self-efficacy (a sense of behavioral control) (Ajzen, 1991). Individuals with more positive attitudes, greater subjective norms, and higher self-efficacy towards the behavior will have a higher likelihood of performing the action. The TPB has been extensively and successfully used to explain a variety of information security behaviors and actions (Bulgurcu et al., 2010; Dinev & Hu, 2007; Guo et al., 2011; Q. Hu et al., 2011; Ifinedo, 2014; Karahanna, Straub, & Chervany, 1999; Peace, Galletta, & Thong, 2003; Siponen et al., 2014; Wynn et al., 2012; Zhang, Reithel, & Li, 2009).

The TPB certainly has limitations, which critics have extensively documented in the literature. For instance, critics have argued that the TPB ignores affective, cognitive, and other biases that impact human behaviors, which means that individuals are not inherently rational in their decision-making (McEachan, Conner, Taylor, & Lawton, 2011). This critique attacks the core assumption (rational decision making) of the TPB. However, Ajzen (2011) argues that many of these confounding factors are included in the definition and measurement of the primary TPB constructs. Furthermore, the TPB does not dictate that individual beliefs are completely free of irrational premises but instead argues that attitudes towards a goal-directed behavior, subjective norms, and a sense of behavioral control follow consistently from those beliefs (Ajzen, 2011; Geraerts et al., 2008).

In the TPB, a sense of behavioral control denotes a belief that individuals have the capability to perform a required action in the face of reasonable obstacles and/or facilitating conditions (Ajzen, 2002). Information security researchers typically use the self-efficacy construct to proxy for an individual's sense of behavioral control (Bulgurcu et al., 2010). Self-efficacy represents individuals' beliefs that they are capable of performing a specific behavior, which means higher self-efficacy results in greater effort to persist in the face of obstacles (Bandura, 1997). In some instantiations of the TPB, this sense of behavioral control is broken down into two antecedents with their own distinctive definitions and measures: (1) self-efficacy and (2) perceived controllability (i.e., beliefs about the extent to which performing the behavior is up to the individual to carry out) (Taylor & Todd, 1995).

Many scholars have pointed out that there are similarities between perceived controllability and self-efficacy (Ajzen, 2002; Bulgurcu et al., 2010). These similarities have led some researchers to use them interchangeably in the behavioral information security literature (Bulgurcu et al., 2010; Tejaswini Herath & H Raghav Rao, 2009; Ifinedo, 2012) and in other disciplines (Fishbein & Cappella, 2006; Fishbein & Yzer, 2003; Yi & Hwang, 2003). In this paper, the argument is presented that whether it is necessary and appropriate to decompose this construct depends on the type of voluntary information security action that is being investigated. For example, individuals' self-efficacy about not reusing passwords across multiple websites may be very high because they feel very capable of following guidelines to generate strong, unique passwords for each website in their own work setting or personal computing environment. Yet, these same individuals may exhibit weak control-related beliefs if they are required to ensure that subordinates or family members (for example) not reuse passwords across multiple websites, because they obviously are not directly involved in coworker or family members' password creation.

In the context of this study, the voluntary adoption of a password manager is an individual decision whereby control-related beliefs are not applicable. There are minimal (if any) control-related obstacles associated with this voluntary adoption, because we are not investigating managers who are responsible for convincing their direct reports (subordinates) to adopt (voluntarily) a password manager. Our context is a self-driven choice, which is effectively captured using the self-efficacy construct.

The attitude construct has arguably received the most attention from behavioral information security researchers. Antecedents for attitudes have been primarily developed using general deterrence theory (D'Arcy, Hovav, & Galletta, 2009; Tejaswini Herath & H. Raghav Rao, 2009), protection motivation theory (Herath & Rao, 2009; Johnston & Warkentin, 2010; Ng, Kankanhalli, & Xu, 2009; Safa et al., 2015; Workman, Bommer, & Straub, 2008; Wynn et al., 2012), and rational choice theory (Bulgurcu et al., 2010; Workman et al., 2008). Attitudes have received all of this attention in the literature because having a positive attitude towards an information security action is consistently one of the most important factors in motivating individuals to adopt voluntary information security controls. Changing individuals' attitudes towards the security behavior is an important first place to start in order to motivate more secure behaviors. Therefore, the focus is on the attitude path in the TPB for this study and how culture may shape individuals' attitudes towards a voluntary security action. How individuals are socialized in specific cultures influences their attitudes because different cultures develop different thought patterns, values, and culturally defined norms towards certain types of behaviors (Christie, Kwon, Stoeberl, & Baumhart, 2003; Schein, 2010; Triandis, 1994).

2.2. Culture

Culture is an abstract construct that often means different things to different scholars. While a complete review of all of the previous definitions of culture is well beyond the scope of this paper, it is necessary to have a base understanding of what is meant by culture in order to fully understand the logical connection among the different constructs proposed in the study. Culture may be delimited at (among others) the group, community, occupation, and national levels (Hofstede, 2001; Triandis, 2000; Trice, 1993). In this paper, the theoretical interest is in national culture differences and uses the following classic definition of national culture:

> Culture consists of patterns, explicit and implicit, of and for behavior acquired and transmitted by symbols, constituting the distinctive achievement of human groups, including their embodiments in artifacts; the essential core of culture consists of traditional (i.e., historically derived and selected) ideas and especially their attached values; culture systems may, on the one hand, be considered as products of action, on the other hand as conditioning elements of further action (Kroeber & Kluckhohn, 1952, p. 181).

The key aspect of this definition of culture as it pertains to this study is *patterns of and for behaviors* and the notion that individuals from different cultural groups exhibit different patterns of thought and behaviors. By this definition, culture plays an important role in determining how groups of people are socialized to behave and think both individually and collectively (O'Reilly III, Chatman, & Caldwell, 1991; Qiu, Lin, & Leung, 2013). Individuals in different parts of the world are socialized via social, political, economic, and educational means to process information differently and, as such, to make sense of the world differently. These cross-cultural differences shape individuals' attitudes towards all types of actions (Christie et al., 2003). Cultural differences are evident in many different dimensions, which are also highly debated in the prior literature.

At the national level, information systems research has most commonly used Hofstede's dimensions of national culture (power distance, uncertainty avoidance, individualism-collectivism, masculinity-femininity, long-term orientation, and indulgence) to measure and theorize about national culture (Kappos & Rivard, 2008; Leidner & Kayworth, 2006). Hofstede (2001) defines each dimensions 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; 6) indulgence refers to the extent to which a culture tries to control their impulses. These dimensions are certainly not the only distinctions between national cultures but these do represent scientifically measured differences that can form a basis for cross-cultural comparisons.

Whereas prior information systems research has explored the potential impact of national culture on IT adoption and implementation for many years (Cardon & Marshall, 2008; Veiga, Floyd, & Dechant, 2001), the behavioral information security literature has just started to investigate the role that national cultural differences play in security related actions (Aurigemma & Mattson, 2018, Chen & Zahedi, 2016; Dinev, Goo, Hu, & Nam, 2009; Dols & Silvius, 2010; Hovav, 2017; Hovav & D'Arcy, 2012; Karjalainen, Siponen, Puhakainen, & Sarker, 2013; Lowry, Posey, Roberts, & Bennett, 2014). For instance, Hovav and D'Arcy (2012) explored the effect of national culture on employee information system misuse 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. More directly germane to this study, Dinev et al. (2009) explored the impact of Hofstede's cultural dimensions as potential model moderators for the TPB towards taking a voluntary recommended security action (use of anti-malware software) among a large group of US and South Korean college students. They found that cultural factors moderated the strength of the relationships in their behavioral model in the context of protective information technologies. These studies, and others, have begun to critically examine and question the universality of human behaviors arguing that individuals from different national cultures can be expected to exhibit different security related behaviors (Aurigemma & Mattson, 2018; Menard, Warkentin & Lowry, 2018). Therefore, there is a 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 LTO cultural dimension was developed specifically to address cross-cultural differences in decision-making (Hofstede, 2001), which makes it a logical extension to the decision oriented TPB. The core idea behind this cultural dimension is that groups of people are socialized to have differing desires in terms of sacrificing time, money, and effort today for potential future success (Cannon, Doney, Mullen, & Petersen, 2010). Cultures that have a longer term orientation value persistence more than immediate results, while cultures that have a shorter term orientation value immediate results and relatively instant gratification (Hofstede, 2001). Previous literature has demonstrated that longer term orientation is positively correlated with being innovative and proactive and negatively correlated with risk taking (Cannon et al., 2010; Vitell et al., 2015; Vitell, Nwachukwu, & Barnes, 1993).

This cultural dimension relates to password managers because of the relatively high setup time and ongoing maintenance time associated with the continued use of password manager applications. That is, password manager adopters invest a significant amount of time in the present in order to spend less time in the future to fix and deal with password related issues. Furthermore, the use of a password manager is a long-term solution to the password management problem. Adopters are choosing to make a short-term investment for a potential future award (not being the subject of an information security breach), which can be argued depends partially on individuals' LTO. Therefore, the following main effect is hypothesized:

H1: Individuals with a long-term relative to a short-term orientation will have a greater intention to adopt a voluntary information security control, specifically password managers.

In the behavioral information security literature that uses the TPB, the attitude path has consistently been demonstrated to be a strong predictor of behavioral intentions (Bulgurcu et al., 2010; Workman et al., 2008). An attitude towards a particular behavior is an individual's overall positive or negative evaluation of the desirability of implementing a behavior (Ajzen, 2001). The desirability of implementing a behavior has also been found to be impacted by cultural norms and values (Lovelock & Yip, 1996; Triandis, 1994). Therefore, it is expected that LTO (a cultural value) will moderate or qualify the impact of attitudes towards adopting voluntary information security actions.

For those individuals with a high (positive) attitude toward adopting a password manager application, it is proffered here that the relationship will be stronger for those with long-term orientation because the long-term orientation will further reinforce the positive attitude towards investing the time and energy to adopt the password manager. Contrarily, for those individuals with a low (negative) attitude toward adopting password manager applications, the prediction is that the effect of long-term orientation will have minimal effect because the effect of attitudes is much stronger than that of LTO construct. In essence, the argument presented in this paper is that an individual's time orientation will not be able to mitigate the effect of the low (negative) attitude towards adopting the voluntary information security control. Therefore, the following qualifying relationship is hypothesized:

H2: An individual's LTO will moderate the effect of attitudes on intentions to adopt a voluntary information security control, specifically password managers.

Figure 1 visually displays both hypotheses.

<< Insert Figure 1 here >>

Figure 1. Research Model for Voluntary Adoption of Information Security Controls

4. Research Design and Method

To empirically test the potential impact of an individual's LTO on taking a voluntary information security action (adopting a password manager) in the context of the TPB, a sequential two-part study of the voluntary adoption (or non-adoption) of a password manager application (LastPass) was conducted. The LastPass password manager application was used because it is a free[1] and

[1] LastPass is actually a freemium product. The primary free features (at the time of our study) included: access on all devices, one-to-one sharing, save and fill passwords, password generators, and multifactor authentication. In addition to these free features, the primary premium (pay) features (at the time of this study) included: one-to-many sharing, advanced multifactor options, emergency access, and priority technical support. In this study, the freemium

well-respected password management application that uses industry-accepted encryption techniques to protect users' account credentials. All of the data in LastPass are secured with AES-256 bit encryption, salted SHA-256 hashing, and PBKDF2 key stretching whereby even LastPass employees cannot view a user's login credentials. Part 1 of the study consisted of presenting all of the subjects with a generic video message about password managers (what they are, what problem they solve, and why they are important) followed by a survey that captured self-reported perceptions of the core TPB constructs including each subject's self-reported behavioral intention to adopt (voluntarily) the LastPass password manager. At this stage of the study, Hofstede's LTO dimension of national culture for each one of our survey participants was also measured. The content and video format of the message was developed and refined 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 were a mix of 50% American and 50% International students of which only three had prior working knowledge of password managers.

The survey was designed and administered using best practices related to question order (pp. 157-165) and instruction wording (pp. 65-105) by Dillman et al. (2014). Additionally, in order to remedy potential common method bias procedurally via the instrument, a proximal separation between the measures of the independent and dependent variables was introduced along with using both positive and negative line items on the survey instrument (Podsakoff, MacKenzie, & Podsakoff, 2012).

Part 2, which occurred one week after the completion of part 1, of the study captured the actual security behavior of the participant (i.e., did they or did they not adopt the password manager). After the participants completed part 1 of our study, they were specifically told that the researchers would be following up with them in one week. In order to alleviate the potential problems associated with a self-reported actual use measure (i.e., social desirability bias resulting in the subjects not being truthful), several questions were asked 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

The study sample consisted of 227 undergraduate business students from a private university in the Midwest portion of the United States with a sizable international population. In return for participation, the subjects were given a small amount of extra credit in their course (between 1 and 2% of their overall course grade depending on the instructor). Our sample was 62% North American, 22% Asian, 10% European, and 6% Middle Eastern. This sample provided adequate variance along the LTO cultural dimension (and the core TPB constructs) to empirically test the proposed relationships. Additionally, the sampling frame used technology extensively in their daily lives, had great familiarity with a variety of online applications (such as social networking sites and school-related information systems), and known to be somewhat carefree with their online privacy and security (Drennan, Sullivan, & Previte, 2006). Furthermore, while the sample

nature of the LastPass password manager was not mentioned by the participants as a reason why they decided to adopt or not to adopt the password manager.

had low adoption rates of password manager applications as reported in the first survey, their overall IT use patterns and large number of password protected online accounts indicated that they would benefit from the voluntarily use of password managers.

4.2.Constructs and Measures

For the survey instrument, measures (items) for the constructs from adapted from pre-validated (reflective) scales taken from previous TPB security and national culture research. Table 1 displays the specific items, citations, and additional details. All items measured reflectively using 7-point Likert scales ranging from (1) strongly disagree to (7) strongly agree (or opposite when the question used reverse scaling).

There is considerable debate in the literature in terms of how to measure national culture (Kirkman, Lowe, & Gibson, 2006; McCoy, Galletta, & King, 2005; Sivakumar & Nakata, 2001). Some scholars argue that culture, particularly Hofstede's dimensions, should be measured at the individual level of analysis (Brockner, 2005; Srite & Karahanna, 2006), whereas other scholars are adamantly opposed to measuring culture at the individual level (Bochner & Hesketh, 1994; Hofstede, 2001; Palich, Horn, & Griffeth, 1995). Much of the contention rests on the definition of Hofstede's dimensions. For instance, if LTO is defined as a property of the culture (i.e., China is a long-term orientation culture), then measuring LTO at the individual level may be misleading. However, if LTO is defined as an individual's perception of the virtues of balancing the past, present, and future, then measuring LTO at the individual level is justified. Srite and Karahanna (2006) argue that it is valid to measure the Hofstede dimensions at the individual-level because individuals interact with many different cultures from all around the world throughout their lives, which 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, the decision was made to follow Srite and Karahanna (2006) and many others and measure the Hofstede dimensions at the individual level.[2]

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

Table 1: Construct Definitions and Measurement Items

<< Insert Table 1 here >>

4.3.Data Analysis Technique

Covariance-based structural equation modeling (CBSEM) was used to evaluate the theorized relationships and overall model fit. CBSEM is considered an appropriate analysis method when testing theoretically derived relationships between latent constructs (Raykov, 2006), which is the case for the proposed research model. Prior to conducting CBSEM analyses, the data was successfully screened for issues that may jeopardize the results, such as outliers, multicollinearity, and non-normality (Byrne, 2001; Kline, 2016).

To test for potential common method variance, the unmeasured latent method factor approach discussed by Podsakoff et al. (2012) was evaluated. In the data, adding this first-order method factor whose only measures were the indicators of the theoretical constructs of interest that shared a common method did not reveal any major issues. However, this approach has been demonstrated to have some weaknesses because it assumes that the method factor does not interact with the trait factors (Richardson, Simmering, & Sturman, 2009). Therefore, as an additional test, the approach of Gefen et al. (2011) used by Moody et al. (2018) was used to test whether the theoretical models fit the data better than models with a single latent factor. In this approach, the single latent factor served as a proxy variable for any common method variance that might be present in our data (Gefen et al., 2011). Across both of these post hoc statistical tests, no was no evidence of common method variance in the 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. Analysis was performed 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 2 displays the measurement item loadings on their respective constructs. All factor loadings were in the range of 0.634 – 0.983. While the recommended threshold for item loadings is 0.7, individual item loadings between .40 and .70 are acceptable for inclusion as long as composite reliabilities are above .70 (which they were for all of the constructs) (Chin, 1998). Average variance extracted (AVE) was also examined to ensure individual item reliability and convergent validity. 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.

Table 2: Confirmatory factor analysis results

<< Insert Table 2 here >>

To assess the discriminant validity of the latent constructs in our research model, AVE, maximum shared squared variance (MSV), and average shared squared variance (ASV) metrics were examined (see Table 2). 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, Black, Babin, & Anderson, 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 reflective indicators of their respective latent constructs. Finally, the model fit for the CFA analysis (which include all latent constructs) was satisfactory ($\chi2$/df = 1.492; CFI = 0.982; SRMR = .0485).

5.2.Structural Model Analysis

Following establishment of the measurement model in the CFA stage, the data was fit to the proposed research model (see Figure 1). Model fit was assessed using multiple criteria (Heck, 1998; Kline, 2016; Raykov, 2006). To further account for the potential impact of even mild deviations from perfectly normal data distributions on the $\chi2$ calculations, Bollen-Stine (1992) bootstrapping was conducted to calculate model fit p-values, which were all above the 0.05 threshold. However, scholars caution against relying upon $\chi2$ measurements alone for model fit determination (Kline, 2016). As such, one goodness-of-fit and one badness-of-fit metric was used to further assess overall model fit.

Comparative fit index (CFI) was used as the goodness-of-fit metric and the standardized root mean square residual (SRMR) as the badness-of-fit metric. The CFI measures model fit relative to a null model and a non-centrality index. The CFI value for the full TPB CBSEM model was above the 0.95 recommended threshold (Hu & Bentler, 1999). The SRMR badness-of-fit metric compares the residuals (unexplained variance) to what would be reasonably expected from a well-fitting model. In the applied research model (the full model displayed in Figure 1), the SRMR was below the common threshold of 0.08, which indicates good model fit (Hu & Bentler, 1999).

Table 3 displays the model fit results and the path coefficients for the three models that were used to empirically evaluate the hypotheses. Model 1 was the TPB only model, which was used to show the effectiveness of the base model. Model 1 showed that all of the core TPB constructs were statistically significant predictors of behavioral intent to adopt LastPass in our sample. Model 2 contained the core TPB constructs along with LTO as a direct antecedent to behavioral intent. In this model, all of the core TPB constructs remained statistically significant, but the main effect of the LTO construct was not statistically significant. Therefore, the direct effect proposed in H1 was not supported in these data.

Model 3 showed an interesting qualifying relationship between attitudes and LTO. Model 3 was the full model with both a direct effect of LTO into behavioral intent and the interaction effect of attitude and LTO. Testing this interaction effect required mean-centering both attitude scores and LTO values across the sample in order to reduce the variance inflation factors associated with testing this interaction effect. Model fit for Model 3 was satisfactory ($\chi2$ / df = 1.474, CFI =

0.982, and SRMR = .0500). This model explained roughly 52.5% of the total variance (SMC = 0.525) of the participant's intent to adopt LastPass. Table 3 shows a modest increase in SMC across models. This increase was primarily attributable to the addition of the main effect of LTO (Model 2) and the attitude by LTO interaction effect (Model 3). While the core LTO dimension of national culture was not a direct significant contributor to LastPass adoption intentions, the effect of attitude towards using a password manager application was qualified by an individual's LTO. The structural path associated with the interaction effect of LTO and attitude was positive and significant ($\beta = 0.137$, $p<0.01$).

Table 3: Structural model analysis results

<< Insert Table 3 >>

To assist in interpreting this qualifying effect, the predicted intention to adopt a password manager as a function of both individuals' attitudes towards adopting and individuals' LTO is plotted (see Figure 2 for the moderating effect of the mean centered variables). For those individuals who had a higher attitude (above average line in Figure 2), the effect of an individual's LTO was positive (i.e., going from short-term to long-term increased behavioral intentions to adopt password managers). Contrarily, for those individuals who had an average or below average attitude (below average line in Figure 2), the effect of long-term orientation was negative (i.e., going from short-term to long-term reduced behavioral intentions to adopt password managers). The differential effect of LTO was greater for those individuals who were more long-term oriented relative to more short-term oriented. Therefore, Model 3 supports the H2 qualifying hypothesis.

<< Insert Figure 2 here >>

Figure 2. Qualifying Effect of Long-term Orientation

5.3.Descriptive Analysis of Actual Adoption

A post-hoc descriptive analysis of actual adoption rates of LastPass was conducted, which provided additional support for the impact of LTO on behavioral intent and actual use of password managers by study participants. Table 4 displays the actual adoption rates for the sample broken down by both attitudes and LTO. Participants with above average LTO values and above average attitudes yielded the highest behavioral intent scores and the highest actual password manager adoption rates. The high long-term orientation and high attitude participants adopted password managers at an overall rate of 24.2%, which is 57% more than the average adoption rate for the whole sample (35 out of 227 or 15.4%). As predicted by the TPB, participants with stronger positive attitudes (high attitude row in Table 4) yielded greater intentions and actual behaviors relative to participants with weaker negative attitudes (low attitude row in Table 4). A chi-square test between LTO (low and high) and attitude (low and high) showed a statistically significant difference (Pearson Chi-square = 7.956, p = 0.005).

Table 4: Actual Use by Long-term Orientation vs Attitude

<< Insert Table 4 here >>

5.4.Effect of the Other Hofstede Dimensions

In this paper, theoretical interest lies in Hofstede's LTO dimension of national culture as it pertains to voluntary information security controls such as password managers that require a sacrifice between short-term time investments with potential long-term benefits. Of the six Hoftsede dimensions of national culture, the LTO dimension is the one that is most applicable to the research context presented in this study. However, all of the Hofstede dimensions were measured using pre-validated scales in the survey instrument. Due to the fact that the data was captured, the main and qualifying effect of the other Hoftsede dimensions (uncertainty avoidance, power distance, individualism-collectivism, masculinity-femininity, and indulgence) were also tested (in an exploratory manner) on attitudes and behavioral intentions to adopt (voluntarily) the LastPass password manager.

None of the attitude by other Hofstede dimensions' interaction effects were statistically significant and none of the main effects were statistically significant. Therefore, in this study, the only Hofstede dimension that had a statistically significant impact on intentions (via the interaction effect of attitudes) to adopt a voluntary information security control was LTO. For a different voluntary information security control, however, different cultural dimensions may be more relevant (Lowry et al., 2014). 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 behavioral intentions, because there is a status dynamic associated with the tailgating threat and control (Aurigemma & Mattson, 2017).

6. Discussion and Conclusion

The prior behavioral information security literature has discovered many important factors such as fear, self-efficacy, attitudes, habits, and norms that influence an individual's propensity to adopt voluntary information security controls (Anderson & Agarwal, 2010; Boss, Galletta, Lowry, Moody, & Polak, 2015; Johnston & Warkentin, 2010). In general, many of the papers in this stream of literature make the implicit or explicit assumption that their theorized relationships will be broadly generalizable (Johnston & Warkentin, 2010; Siponen & Tsohou, Forthcoming). That is, much of the prior literature speculates or assumes that their reported findings will be robust to individuals across different cultures, genders, socio-economic backgrounds, and educational levels.

However, individuals socialized in different cultures have varying values, beliefs, and thought patterns across multiple cultural dimensions (Hofstede, 2001; Triandis, 2000), which may positively or negatively influence their propensity to adopt voluntary information security controls (Aurigemma & Mattson, 2018; Chen & Zahedi, 2016, Menard, Warkentin & Lowry, 2018). One cultural dimension that is particularly relevant to the voluntary adoption of information security controls (particularly those requiring relatively high up-front setup costs) is LTO (Hofstede, 2001; Spears, Xiaohua, & Mowen, 2001).

In this study, LTO did not have a direct impact on behavioral intent or the actual adoption rates of LastPass. However, the data analysis did reveal a qualifying effect of LTO on attitudes towards intention to adopt (voluntarily) password managers. The effect of positive attitudes increased when individuals were more long-term oriented but the effect was reversed for average and negative attitudes. This would suggest that having a shorter term orientation can suppress some of the negative impact that negative attitudes have towards adopting a password manager application. In terms of actual adoption, individuals with high LTO and strong positive attitudes adopted password manager applications 57% more than the average adoption rate across our sample. The implication of this finding is that a one-size-fits-all approach to encourage voluntary information security actions (or intentions thereof) may not be the best approach, because individuals from different cultures have varying beliefs and values along many dimensions including (but not limited to) time orientation. As such, security awareness and training messages should account for individuals with both short and long term orientation. Those with short term orientation should be more moved by messages that espouse the immediate positive impact of using a password manager (with possible instant gratification helping to overcome neutral or poor attitudes toward the behavior). In contrast, security messages that impart sustained improvements and benefits of better account management through the use of tools such as password managers should provide greater impact to those with long term orientations.

One of the goals of this paper was to discover behavioral antecedents to encourage individuals to use better password management strategies through the implementation of password manager applications. However, password manager applications are not the only solution to poor password management. Federated systems such as Google or Facebook where a user logs into one system and is granted access to multiple other systems also aims to solve the problems that individuals have regarding password management. We believe that it is not realistic to have a single federated system that manages access across all platforms and to all banks, social sites, email accounts, and others, but the popularity of platform oriented websites like Google, Facebook, and Yahoo may make federated systems part of the solution. Interestingly, the initially high setup costs in terms of time and effort associated with adopting password managers are much less for many federated systems, which may impact the effect of LTO. Therefore, an interesting future study would be to test the findings of this study model using a federated system. It would not be surprising if the results are different because each solution requires a different set of short-term costs and long-term benefits.

Like all research, this study has limitations. First, the behavioral information security literature has decomposed the attitude construct into a multi-dimensional construct. Antecedents for attitudes include (among others) the core elements of rational choice theory and general deterrence theory (Bulgurcu et al., 2010; D'Arcy et al., 2009; Tejaswini Herath & H. Raghav Rao, 2009; Workman et al., 2008). We did not test the effects of LTO “downstream” and our model only included the higher order attitude construct. Decomposing attitudes might reveal additional insights into the effects of LTO and might be an interesting area for future research. Second, LTO effects were only investigated the in connection with the TPB. As previously mentioned, there is no consensus among behavioral information security researchers as to which theoretical approach is best and under which conditions. Therefore, future research can investigate the effect of LTO (and other cultural dimensions) in other models such as the PMT, GDT, or psychological capital. Third, although there was significant variance of the LTO construct for the survey participants to test tje proposed research model, the sample did not include any participants from the most short-term oriented cultures. It is possible that the main effect of LTO will be significant if we had subjects from Ghana or Nigeria, for example. Therefore, future research might focus on the shortest of the short-term oriented cultures to further empirically test our theorized relationships.

The main practical contribution of this study, as with most other research associated with cultural dimensions and human behaviors, is that it is important to know the composition and behavioral orientations of the people involved. In the university where the data for this study was collected, for example, basic security awareness training and documentation is 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. As succinctly argued by Karjalainen et al. (2013), “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 organizations or social settings where there is a diverse cultural background of people that are relied upon to take sound and effective security actions, ignoring the effect of cultural dimensions such as LTO, and possibly other cultural characteristics, can have a deleterious impact on the overall organizational information security posture.

References

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

Ajzen, I. (2001). Nature and operation of attitudes. *Annual review of psychology, 52*(1), 27-58.

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. *Journal of Applied Social Psychology, 32*(4), 665-683.

Ajzen, I. (2011). The theory of planned behaviour: reactions and reflections. *Psychology & health, 26*(9), 1113-1127.

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

Aurigemma, S. (2013). A Composite Framework for Behavioral Compliance with Information Security Policies. *Journal of Organizational and End User Computing, 25*(3), 32-51.

Aurigemma, S., & Mattson, T. (2017). Privilege of Procedure: Evaluating the Effect of Employee Status on Intent to Comply with Socially Interactive Information Security Threats and Controls. *Computers & Security, 66*(1), 218-234.

Aurigemma, S. and T. Mattson (2018). Exploring the Effect of Uncertainty Avoidance on Taking Voluntary Protective Security Actions. *Computers & Security*, 73, 219-234.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational behavior and human decision processes, 50*(2), 248-287.

Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*. New York: W. H. Freeman and Company.

Beardsley, T., Hodgman, R., Hart, J., & Geiger, H. (2016). *The Attacker's Dictionary: Auditing Criminal Credential Attacks*. Retrieved from https://community.rapid7.com/community/infosec/blog/2016/03/01/the-attackers-dictionary

Bochner, S., & Hesketh, B. (1994). Power Distance, Individualism/Collectivism, and Job-Related Attitudes in a Culturally Diverse Work Group. *Journal of Cross-Cultural Psychology, 25*(2), 233-257.

Bollen, K. A., & Stine, R. A. (1992). Bootstrapping Goodness-Of-Fit Measures in Structural Equation Models. *Sociological Methods & Research, 21*(2), 205-229.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly, 39*(4), 837-864.

Brockner, J. (2005). Unpacking Country Effects: on the Need to Operationalize the Psychological Determinants of Cross-National Differences. In B. M. Staw & R. L. Sutton (Eds.), *Research in Organizational Behavior* (pp. 335-369). Greenwich, CT: JAI Press.

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

Byrne, B. M. (2001). Structural Equation Modeling with AMOS, EQS, and LISREL: Comparative Approaches to Testing for the Factorial Validity of a Measuring Instrument. *International Journal of Testing, 1*(1), 55-86.

Cannon, J. P., Doney, P. M., Mullen, M. R., & Petersen, K. J. (2010). Building Long-Term Orientation in Buyer-Supplier Relationships: The Moderating Role of Culture. *Journal of Operations Management, 28*(6), 506-521.

Cardon, P. W., & Marshall, B. A. (2008). National Culture and Technology Acceptance: The Impact of Uncertainty Avoidance. *Issues in Information Systems, 9*(2), 103-110.

Chen, Y., & Zahedi, F. M. (2016). Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China. *MIS Quarterly, 40*(1), 205-222.

Chin, W. W. (1998). Commentary: Issues and Opinion on Structural Equation Modeling. *MIS Quarterly, 22*(1), vii-xvi.

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

Christie, M. J., Kwon, I.-W. G., Stoeberl, P. A., & Baumhart, R. (2003). A Cross-Cultural Comparison of Ethical Attitudes of Business Managers: India, Korea and the United Staes. *Journal of Business Ethics, 46*(3), 263-287.

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

CSID. (2012). *Consumer Survey: Password Habits - A study of password habits among American consumers*. Retrieved from https://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf

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.

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386.

Dols, T., & Silvius, A. (2010). Exploring the Influence of National Cultures on Non-Compliance Behavior. *Communications of the IIMA, 10*(3).

Drennan, J., Sullivan, G. M., & Previte, J. (2006). Privacy, Risk Perception, and Expert Online Behavior: An Exploratory Study of Household End Users. *Journal of Organizational and End User Computing, 18*(1), 1-22.

Fishbein, M., & Cappella, J. N. (2006). The role of theory in developing effective health communications. *Journal of Communication, 56*(s1), S1-S17.

Fishbein, M., & Yzer, M. C. (2003). Using theory to design effective health behavior interventions. *Communication Theory, 13*(2), 164-183.

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

Gefen, D., Straub, D. W., & Rigdon, E. E. (2011). An Update and Extension to SEM Guidelines for Admnistrative and Social Science Research. *MIS Quarterly, 35*(2), iii-xiv.

Geraerts, E., Bernstein, D. M., Merckelbach, H., Linders, C., Raymaekers, L., & Loftus, E. F. (2008). Lasting false beliefs and their behavioral consequences. *Psychological Science, 19*(8), 749-753.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis: A Global Perspective*. Upper Saddle River, NJ: Pearson.

Heck, R. H. (1998). Factor Analysis: Exploratory and Confirmatory Approaches. In G. Marcoulides (Ed.), *Modern Methods for Business Research* (pp. 177-215). Mahwah, NJ: Erlbaum.

Herath, T., & Rao, H. R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems, 47*(2), 154-165.

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

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations*. Thousand Oaks, CA: Sage.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). Cultures and organizations: Software of the mind. Revised and expanded. *McGraw-Hill, New York*.

Hovav, A. (2017). *How Espoused Culture Influences Misuse Intention: A Micro-Institutional Theory Perspective.* Paper presented at the Proceedings of the 50th Hawaii International Conference on System Sciences.

Hovav, A., & D'Arcy, J. (2012). Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the US and South Korea. *Information & Management, 49*(2), 99-110.

Hu, L., & Bentler, P. M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives. *Structural Equation Modeling, 6*(1), 1-55.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

Humphries, D. (2015). *Best Practices for Workplace Passwords*. Retrieved from http://www.softwareadvice.com/security/industryview/password-workplace-report-2015/

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

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *computers & security, 31*(1), 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79.

Jarvis, C. B., Mackenzie, S. B., & Podsakoff, P. M. (2003). A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research, 30*(2), 199-218.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549-566.

Kappos, A., & Rivard, S. (2008). A Three-Perspective Model of Culture, Information Systems, and Their Development and Use. *MIS Quarterly, 32*(3), 601-634.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly, 23*(2), 183-213.

Karjalainen, M., Siponen, M. T., Puhakainen, P., & Sarker, S. (2013). *One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions.* Paper presented at the PACIS.

Kirkman, B. L., Lowe, K. B., & Gibson, C. B. (2006). A Quarter Century of "Culture's Consequences": A Review of Empirical Research. *Journal of International Business Studies, 37*(3), 285-320.

Kline, R. B. (2016). *Principles and Practice of Structural Equation Modeling: Fourth Edition*. New York, NY: Guilford Press.

Kroeber, A. L., & Kluckhohn, C. (1952). *Culture: A Critical Review of Concepts and Definitions*. Cambridge, Mass: The Museum.

Leidner, D. E., & Kayworth, T. (2006). A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly, 30*(2), 357-399.

Liu, Y.-T., Chen, H.-B., Zang, B.-Y., & Liang, Z. (2018). SplitPass: A Mutually Distrusting Two-Party Password Manager. *Journal of Computer Science and Technology, 33*(1), 98-115.

Lovelock, C. H., & Yip, G. S. (1996). Developing Global Strategies for Service Businesses. *California Management Review, 38*(2), 64-86.

Lowry, P. B., Posey, C., Roberts, T. L., & Bennett, R. J. (2014). Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse. *Journal of Business Ethics, 121*(3), 385-401.

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, 75, 147-166.

McCoy, S., Galletta, D. F., & King, W. R. (2005). Integrating National Culture into IS Research: The Need for Current Individual Level Measures. *Communications of the Association for Information Systems, 15*.

McEachan, R. R. C., Conner, M., Taylor, N. J., & Lawton, R. J. (2011). Prospective prediction of health-related behaviours with the Theory of Planned Behaviour: a meta-analysis. *Health Psychology Review, 5*(2), 97-144.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Security Policy Compliance. *MIS Quarterly, 42*(X), 1-XX.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems, 46*(4), 815-825.

O'Reilly III, C. A., Chatman, J., & Caldwell, D. F. (1991). People and Organizational Culture: A Profile Comparison Approach to Assessing Person-Organization Fit. *Academy of Management Journal, 34*(3), 487-516.

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

Palich, L. E., Horn, P. W., & Griffeth, R. W. (1995). Managing in the International Context: testing Cultural Generality of Sources of Commitment to Multinational Enterprises. *Journal of Management, 21*(4), 671-690.

Peace, A. G., Galletta, D. F., & Thong, J. Y. (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems, 20*(1), 153-178.

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

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of Method Bias in Social Science Research and Recommendations on How to Control It. *Annual Review of Psychology, 63*(1), 539-569.

Qiu, L., Lin, H., & Leung, A. K.-y. (2013). Cultural Differences and Switching of In-Group Sharing Behavior Between an American (Facebook) and a Chinese (Renren) Social Networking Site. *Journal of Cross-Cultural Psychology, 44*(1), 106-121.

Raykov, T., & Marcoulides, G.A. (2006). *A First Course in Structural Equation Modeling*. Mahwah, NY: Lawrence Erlbaum.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A Tale of Three Perspectives: Examining Post Hoc Statistical Techniques for Detection and Correction of Common Method Variance. *Organizational Research Methods, 12*(4), 762-800.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organizations. *Computers & Security, 53*, 65-78.

Schein, E. H. (2010). *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.

Siponen, M., Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Siponen, M., & Tsohou, A. (Forthcoming). Demystifying the Influence IS Legends of "Positivism". *Journal of the Association for Information Systems*.

Sivakumar, K., & Nakata, C. (2001). The Stampede toward Hofstede's Framework: Avoiding the Sample Design Pit in Cross-Cultural Research. *Journal of International Business Studies, 32*(3), 555-574.

Spears, N., Xiaohua, L., & Mowen, J. C. (2001). Time Orientation in the United States, China, and Mexico: Measurement and Insights for Promotional Strategy. *Journal of International Consumer Marketing, 13*(1), 57-75.

Srite, M., & Karahanna, E. (2006). The Role of Espoused National Cultural Values in Technology Acceptance. *MIS Quarterly, 30*(3), 679-704.

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

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

Triandis, H. C. (1994). *Culture and Social Behavior*. New York: McGraw-Hill, Inc.

Triandis, H. C. (2000). Culture and Conflict. *International Journal of Psychology, 35*(2), 145-152.

Trice, H. M. (1993). *Occupational Subcultures in the Workplace*. Ithaca, NY: ILR Press.

Veiga, J. F., Floyd, S., & Dechant, K. (2001). Towards modelling the effects of national culture on IT implementation and acceptance. *Journal of Information technology, 16*(3), 145-158.

Vitell, S. J., King, R. A., Howie, K., Toti, J.-F., Albert, L., Hidalgo, E. R., & Yacout, O. (2015). Spirituality, Moral Identity, and Consumer Ethics: A Multi-cultural Study. *Journal of Business Ethics, 139*(1), 147-160.

Vitell, S. J., Nwachukwu, S. L., & Barnes, J. H. (1993). The Effects of Culture on Ethical Decision-Making: An Application of Hoftsede's Typology. *Journal of Business Ethics, 12*(10), 753-760.

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

Wynn, D., Williams, C., Karahanna, E., & Madupalli, R. (2012). *Preventive Adoption of Information Security Behaviors*. Paper presented at the Thirty Third International Conference on Information Systems, Orlando, FL December 16-19.

Yi, M. Y., & Hwang, Y. (2003). Predicting the use of web-based information systems: self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model. *International journal of human-computer studies, 59*(4), 431-449.

Yoo, B., Donthu, N., & Lenartowicz, T. (2011). Measuring Hofstede's five dimensions of cultural values at the individual level: Development and validation of CVSCALE. *Journal of International Consumer Marketing, 23*(3-4), 193-210.

Zeltser, L. (2015). *Password Managers*. Retrieved from https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201310_en.pdf

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of Perceived Technical Protection on Security Behaviors. *Information Management & Computer Security, 17*(4), 330-340.

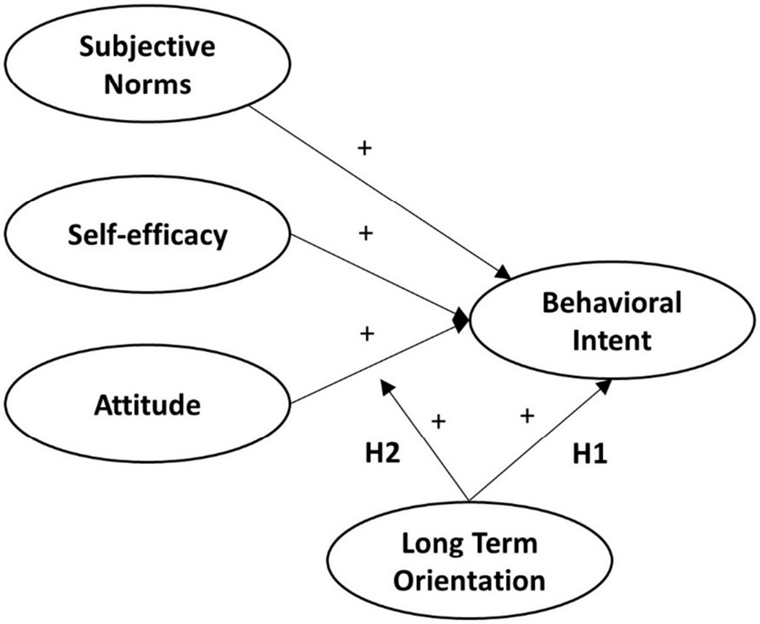

Figure 1: Research Model for Voluntary Adoption of Information Security Controls

Table 1: Construct Definitions and Measurement Items

				Factor		Std
Construct	**Definition and Item Source(s)**	**Survey Question/Measurement Item**	**Item**	**Load**	**Mean**	**Dev**
Behavioral Intent	Self-reported intention to perform a security-related behavior. Items adapted from Ajzen (1991), Bulgurcu et al. (2010)	I intend to use a password manager in the next week.	BINT1	0.927	4.11	1.538
		I predict I will use a password manager in the next week.	BINT2	0.983	4.05	1.536
		I plan to use a password manager in the next week.	BINT3	0.908	4.16	1.524
Subjective Norms	The perceived social pressure to engage or not to engage in a security-related behavior. Items adapted from Taylor and Todd (1995), Tejaswini Herath and H Raghav Rao (2009)	My peers think I should use a password manager application to help protect my online account passwords.	SNORM1	0.869	3.88	1.439
		Those senior to me (parents, professors, bosses, etc.) think I should use a password manager application to help protect my online account passwords.	SNORM2	0.676	4.29	1.561
		Those subordinate / junior to me think I should use a password manager application to help protect my online account passwords.	SNORM3	0.869	3.88	1.408
Self-efficacy	One's perceived ability to successfully complete a security-related behavior. Items adapted from Bandura (1991); Tejaswini Herath and H Raghav Rao (2009)	Password manager software is easy to use.	SE1	0.809	5.29	1.091
		Password manager software is convenient to use.	SE2	0.837	5.13	1.185
		I am able to use password software without much effort.	SE3	0.799	5.10	1.197
Attitude	The self-reported degree to which performance of a security behavior is positively or negatively valued. Items adapted from Ajzen (1991); Tejaswini Herath and H Raghav Rao (2009)	Password manager software is easy to use.	ATT1	0.773	5.06	1.141
		Password manager software is convenient to use.	ATT2	.0964	5.28	1.064
		I am able to use password software without much effort.	ATT3	0.872	5.33	1.057
Long-term Orientation	The self-reported degree to which one prefers long-term values and traditions vs quick gratification and short-term needs. Items adapted from Hofstede, Hofstede, and Minkov (2010); Yoo, Donthu, and Lenartowicz (2011)	I plan for the long term.	LTO1	0.634	5.36	1.179
		I work hard for success in the future.	LTO2	0.867	6.00	1.075
		Persistence is important to me.	LTO3	0.739	5.84	1.037

Table 2: Confirmatory factor analysis results

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, BINT = behavioral intent, SEFF = self-efficacy, ATT = Attitude, LTO = long term orientation

Table 3: Structural model analysis results

SEM Model Fit Results	Model 1	Model 2	Model 3
χ2 / df	1.661	1.427	1.474
χ2	79.705	111.317	198.67
df	48	78	88
Comparative Fit Index (CFI)	0.984	0.985	0.982
Standardized Root Mean Residual (SRMR)	0.048	0.0489	0.05
Squared Multiple Correlation (SMC)	0.506	0.514	0.525
SEM Structural Path Results			
SNORM → BINT	0.471***	0.465***	0.458***
SEFF → BINT	0.238***	0.249***	0.247***
ATT → BINT	0.229***	0.241***	0.237***
LTO → BINT	[redacted]	NS	NS
LTO x ATT Interaction → BINT	[redacted]	[redacted]	0.137**

Note: **p<0.01, ***p<0.001 BINT = behavioral intent, SEFF = self-efficacy, ATT = Attitude, LTO = long-term orientation, NS = not significant

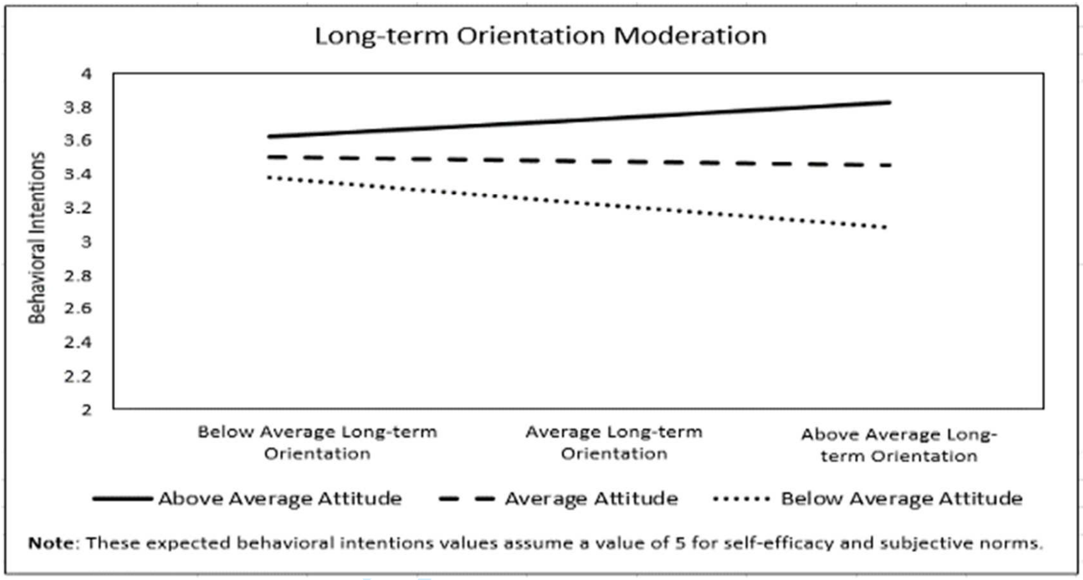

Figure 2. Qualifying Effect of Long-term Orientation

Table 4: Actual Use by Long-term Orientation vs Attitude

	Low LTO	**High LTO**	
# of Participants	68	55	**Low ATT**
Mean BINT	3.78	3.25	
% Actual Behavior	11.80%	2%	
# of Participants	38	66	**High ATT**
Mean BINT	4.47	4.96	
% Actual Behavior	18.40%	24.20%	

BINT = behavioral intent, ATT = Attitude, LTO = long-term orientation, Actual Behavior means adopted use of a password manager as a result of participating in this study