COMPUTERS & SECURITY 73 (2018) 219–234

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/

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