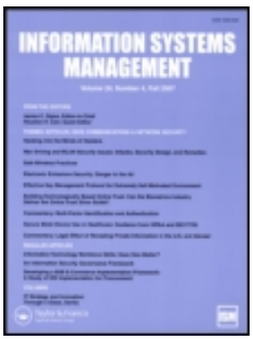

Information Systems Management

ISSN: 1058-0530 (Print) 1934-8703 (Online) Journal homepage: http://www.tandfonline.com/loi/uism20

Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective

Bartlomiej Hanus & Yu "Andy" Wu

To cite this article: Bartlomiej Hanus & Yu "Andy" Wu (2016) Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective, Information Systems Management, 33:1, 2-16, DOI: 10.1080/10580530.2015.1117842

To link to this article: https://doi.org/10.1080/10580530.2015.1117842

Accepted author version posted online: 30 Nov 2015.
Published online: 30 Nov 2015.

INFORMATION SYSTEMS MANAGEMENT
2016, VOL. 33, NO. 1, 2–16
http://dx.doi.org/10.1080/10580530.2015.1117842

Taylor & Francis
Taylor & Francis Group

Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective

Bartlomiej Hanus[a] and Yu "Andy" Wu[b]

[a]School of Business, Emporia State University, Emporia, Kansas, USA; [b]College of Business, University of North Texas, Denton, Texas, USA

ABSTRACT
This article uses the protection motivation theory to study the impact of information security awareness on desktop security behavior. It contributes to the literature by examining the roles played by awareness, an important antecedent to the cognitive processes in the protection motivation theory. The findings indicate that security awareness significantly affects perceived severity, response efficacy, self-efficacy, and response cost. Constructs in the coping appraisal process (except response cost), in turn, significantly impact recommended security behavior.

KEYWORDS
Information security awareness; protection motivation theory; countermeasures; threats

Introduction

Information security of home users is an extremely important area of information security. While the majority of studies focus on behaviors of individuals within organizational settings, those behaviors are indirectly influenced by the practice of security protection by home users. Unfortunately, compared with studies of organizational user behaviors, the current security literature lacks examination of how home users deal with information security threats.

Information security is a broad field with a number of subareas. The subject matter of this study is a specific subarea—desktop security. We define desktop security as the protection of equipment and data stored on home users' desktop or laptop computers, as well as the recovery from potential attacks. This is distinct from other security subareas, e.g., wireless security, passwords, etc. Even today, most of the cybercrimes are still related to desktop security. According to Norton Cybercrime Report (Symantec, 2012), 46% of the computer users globally have fallen victim to some sort of computer virus or malware attack, 40% do not know that malware can act in a discreet manner, making it difficult to recognize if a computer has been compromised. Furthermore, it is estimated that more than half of individuals are not absolutely sure whether their computers are free of viruses, and almost one third of people do not understand the risks associated with not sufficiently protecting themselves online. What is more interesting, however, is the fact that 69% of the people do not back up their data on a regular basis. Furthermore, McAfee Labs (2010) reports that although other security threats increase faster, malware continues to be the biggest threat for both corporate and home users. Just in the first three quarters of 2010 the company was able to identify over 14 million unique pieces of malware, which is over a million more than the number of unique malware for the comparable period in 2009. This tendency is also supported by Shimeall (2002), who observed that the sophistication of attacker tools has been increasing for the past 20 years, while at the same time it requires less and less technical knowledge to perform these attacks. Nowadays, many of these hacker tools are freely available to download, and require little or no knowledge to use them. Another trend that clearly adds to potential security issues is that client-side software remains unpatched. Even though software vendors often provide fixes for client-side vulnerabilities, users often do not apply these security patches in a timely manner. This applies to both the operating systems and the applications installed on these systems (SANS Institute, 2010). Among the various areas in information security (Ciampa, 2010), desktop security presents a serious threat to information security because no matter how much time and effort is spent on information security, it is only as good as its weakest link. Unfortunately, usually it is people who are the weakest link (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Hinde, 2001; Kumar, Mohan, & Holowczak, 2008). Therefore, regardless of all technological developments

CONTACT Bartlomiej Hanus bartlomiejh@gmail.com School of Business, Emporia State University, 1 Kellogg Circle, Campus Box 4039 Emporia, KS 66801, USA.

in information security, educating users and making them aware of these developments remains an important factor in information security (Albrechtsen & Hovden, 2010; Dhillon & Backhouse, 2001; Straub & Welke, 1998). However, the current body of information security knowledge is primarily focused on the Internet security of home users (LaRose, Rifon, & Enbody, 2008), ignoring the importance of desktop security with only some exceptions (Crossler, 2010). We, therefore, focused on home user desktop security issues, as its importance should not be underestimated (SANS Institute, 2010; Symantec, 2010).

This study contributes to the literature by applying the protection motivation theory (PMT) to investigate home users' security behaviors to protect desktop security. Another contribution is to go beyond the nomological model of the PMT and examine the roles played by awareness, an important antecedent to the central constructs in the PMT. PMT (Rogers, 1975) has its origins in research related to fear appeals that is primarily focused on how fear-arousing communication can influence attitudes and subsequent behavior. PMT addresses the issue by decomposing fear appeals into multidimensional components that would allow the researchers to determine common variables affecting attitudinal change (Milne, Sheeran, & Orbell, 2000). Such cognitive processes take the forms of threat appraisal (i.e., perceptions of how threatened a person feels he or she is) and coping appraisal (i.e., perceptions of the recommended coping response to the aforementioned threat). In addition to explicating the roles of awareness, we divide awareness, which has been typically presented as a monolithic construct, into two types: threat awareness (TA) and countermeasure awareness (CA). Such division richly informs us about how awareness exactly exerts its influence on users' security behaviors.

Improvement in desktop security behaviors (DSBs) is commonly a goal of security awareness training. With the training, users are expected to understand and identify security risks in the context of their interactions with information systems, and know what actions reduce those risks (Herold, 2010). Thus, successful security training should result in increased consciousness of protective behaviors (Peltier, 2000). However, security awareness is very different from other security topics. It is the least "technical" one from the computer science and engineering perspectives (Dunlop & Kling, 1992). That might also be the reason why sometimes it is overlooked by more technically-oriented security experts. However, high information security awareness can be the most cost-effective solution to problems (Peltier, 2000), as it allows individuals to adopt a more preventive and proactive approach rather than a reactive one. To the best of our knowledge, although there has been an abundant discussion of the relationship between security awareness and behaviors in the practitioner literature, academic examination of this relationship still is not sufficient. This article makes a contribution by dissecting the two major components of awareness, that of threats and that of countermeasures, and examining their influence on user security as related to the PMT (Maddux & Rogers, 1983; Rogers, 1975).

In addition, the current literature on the topic reveals that, although lack of security awareness among individuals has been widely studied, it is primarily focused on organizational determinants of user compliance with security policies and avoidance of security threats (Herath & Rao, 2009; Pahnila, Siponen, & Mahmood, 2007; Vance, Siponen, & Pahnila, 2012; Warkentin, Malimage, & Malimage, 2012). Moreover, present research implementations of the PMT focus mostly on the cognitive mediating processes responsible for formation of protection motivation, as well as subsequent behavioral intentions. At the same time, the antecedents of threat and coping appraisals are frequently omitted, even though the original literature on the PMT emphasizes the importance of the sources of information based on which individuals assess the magnitude of threats and their respective abilities to address such threats (Milne et al., 2000). This article aims at filling this significant gap in research and examines the effect of desktop security awareness on threat and coping appraisals, and subsequent behaviors.

The remainder of the article is organized as follows. First, the relevant background literature is reviewed. Next, the research model for this study, its constructs, and hypotheses are proposed, followed by the discussion of research methodology and measurement scales that were employed in this study. Finally, the results of data analyses are presented, along with implications and possible limitations.

Literature review

Information security awareness is an individual's knowledge of particular security threats and the potential countermeasures against those threats (Siponen, 2000; Thomson & von Solms, 1998). This perspective on awareness has been introduced by Talib, Clarke, and Furnell (2010) to analyze information security awareness within home and work environments. Information security can be classified as protective technology, whose purpose is to protect users from effects of

negative technologies, e.g., all sort of malware (Dinev & Hu, 2007). Accordingly, Siponen (2000) defined information security awareness as a "state where users in an organization are aware of—ideally committed to—their security mission (often expressed as in end-user security guidelines)" (p. 31). Although this definition is directed toward organizational environments, it still is useful in an individual user context. An important part of it is the user commitment to security. Siponen's understanding of commitment is based on Senge (1994), which treats organization as a system. Since the society can also be treated as a system (Parsons, 1991), Siponen's definition can be easily extrapolated toward individual users, members of the society who might be committed not only to their individual interests, but also to the common interest of the whole. What is more, such commitment could be conceptualized through Dinev and Hu's (2007) approach to technology awareness—an increased consciousness of and interest in learning about technological problems (2007). Thus, "anyone who regards information in any form as an important asset … should be aware of the possible threats related to it" (Siponen, 2001, p. 24).

Therefore, it is appropriate to treat information security awareness from the protective technology point of view and perceive information security as a necessity rather than a benefit. Parallels can be drawn between security behaviors and preventive actions in healthcare, whose goal is to prevent or minimize risks of diseases (Jayanti & Burns, 1998). There are two approaches in security literature that employ this standpoint. The first is based on the health belief model (Rosenstock, 1966). Ng, Kankanhalli, and Xu (2009) used a modified health belief model in their study about exercising care with email attachments, and explained that it is relevant in security context because of the preventive nature of security practices. They found that perceived susceptibility, perceived benefits, and self-efficacy (SE) are determinants of computer security behavior.

The second approach to information security from the protective technology perspective draws upon the PMT (Rogers, 1975). The PMT is built on the anticipation of a negative outcome in one's health and the desire to minimize the outcome, which leads to one being motivated to self-protect (Weinstein, 1993). Similarly in information security, one is motivated to practice information security to avoid security threats. In general, the PMT involves two processes—threat appraisal and coping appraisal—that are used to explain behavior. Threat appraisal consists of perceived vulnerability (PV) and perceived severity (PS). The former is the probability of occurrence of a negative event while the latter is the size of the potential consequence, should the negative event occur. Nonetheless, both constructs are similar in nature to severity and susceptibility in health belief model, except that the PMT pays less attention to emotional arousal caused by severity (Prentice-Dunn & Rogers, 1986), and that susceptibility in health belief model includes not only the particular threat under study but also susceptibility to threats in general (Becker, 1974). Coping appraisal includes response efficacy (RE), SE, and response cost (RC). RE can be defined as one's confidence that certain type of behaviors will allow him or her to avoid or minimize the risk of negative event.

In this study we choose to implement the PMT approach over the health belief model due to a number of reasons. First, according to Prentice-Dunn and Rogers (1986), the components shared by both models are structured into the threat appraisal and coping appraisal constructs in the PMT, which helps to understand how people perceive threats and how they cope with them. Second, the original health belief model did not include the SE component (Rosenstock, 1966). Furthermore, according to Rogers (1983), the health belief model often does not account for the frequent lack of effects of severity and vulnerability, while the PMT posits that they will either have no effect or a boomerang effect when SE and RE are low. Third, the health belief model assumes that presence of cues to action should trigger the appropriate health behaviors. This causes ambiguity around the mechanism through which model components are converted into actual behavior (Prentice-Dunn & Rogers, 1986). Fourth, Prentice-Dunn and Rogers (1986) suggested that the PMT applies to a broader context of threat than health belief model. Therefore, the PMT is a more comprehensive approach to studying DSBs. Finally, the PMT has a significant advantage over other competing theories in that it has been consistently tested through experimental studies (Milne et al., 2000).

Even though the PMT has been widely implemented to investigate various aspects of information security, researchers' attention has been mostly paid to organizational issues. The present research addresses security awareness and behavior in home settings of individual users. Home users are vulnerable to security threats equally if not more than organizational users. While such vulnerability can be caused by many factors, lack of awareness is considered one of the primary issues among them (James, Nottingham, & Kim, 2013; Kritzinger & von Solms, 2010). The key distinction is that an organization can directly impact individuals' security awareness through security awareness and training programs (Puhakainen & Siponen, 2010),

while home users' awareness often depends on their own initiatives (James et al., 2013). As of current, only several studies (Crossler, 2010; Gurung, Luo, & Liao, 2009; LaRose et al., 2008; Liang & Xue, 2010; Woon, Tan, & Low, 2005) in information security have implemented the PMT framework to investigate individual behaviors or behavioral intentions with regards to protection from security threats. Their results, however, deliver inconclusive results on the significance of the formation of protection motivation mechanisms among home users. For example, Crossler's (2010) study of data backup practices concludes that individuals who feel vulnerable to threats they perceive as severe are less likely to engage in protective behaviors. Crossler's interpretation of such counterintuitive results suggests that threat appraisal mechanisms may actually be the antecedents of coping appraisal, which is consistent with some of the literature on the topic (Witte, Cameron, McKeon, & Berkowitz, 1996). LaRose et al. (2008) suggest that the perceived magnitude of a threat can generate intense fear, which in turn can inhibit the implementation of protective behaviors. Woon et al. (2005) found that when it comes to enabling security features in home wireless networks, PV is not a significant predictor of recommended behavior. On the other hand, the literature on threat appraisal mechanisms as determinants of using anti-spyware software on home computer provides inconclusive evidence (Gurung et al., 2009; Liang & Xue, 2010). Therefore, it is worthwhile to further investigate the PMT threat appraisal process in home user security settings. At the same time, researchers on the topic consistently confirm the positive (and significant) effect of two of the three elements of coping appraisal—SE and RE. However, the effect of RC on behavior (behavioral intentions) remains an unanswered question. Although the literature generally agrees that it should act as a behavior inhibitor, it also reports mixed results about its significance in explaining human behavior (Crossler, 2010; Liang & Xue, 2010; Woon et al., 2005) or omits the problem (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010).

The review of the literature also reveals that antecedents of threat and coping appraisals for home users have not been investigated yet, even though the importance of sources of information that individuals draw upon to assess threats should not be underestimated (Milne et al., 2000). The threat and coping appraisal processes do not occur without any basis, and one critical factor that influences the formation of cognitive processes in the PMT is prior experience (Maddux & Rogers, 1983; Milne et al., 2000; Rogers, 1975, 1983). In the context of desktop security, prior experience may include users' exposure to threats and countermeasures through sources that are formal (e.g., awareness education campaigns, or training) or informal (vicarious experience related by family members, friends, media, and so on). Thus, awareness of threats and their respective countermeasures are very likely to have bearings on the cognitive processes appraising the threats and coping strategies. The present study addresses a significant gap in literature by examining awareness as an antecedent to the appraisal and coping constructs in the PMT.

Research model and hypotheses

The research model for this study (Figure 1) is based on a modified version of the PMT used by previous studies in explaining security behaviors (Crossler, 2010; LaRose et al., 2008; Liang & Xue, 2010; Woon et al., 2005). It contributes to our understanding of security awareness by testing the PMT-based relationships in the settings of desktop security awareness, an area that has not been studied intensively in the extant literature, despite its importance. Our model introduces two important new constructs: TA and CA, exemplifying important sources of information that are the basis for individuals' perceptions of threats and countermeasures (Milne et al., 2000; Witte et al., 1996). The model also conceptualizes how the awareness constructs impact PS, PV, RE, SE, RC, and, in turn, DSB. The relationships among the constructs are based on the original literature on the PMT (Maddux & Rogers, 1983; Prentice-Dunn & Rogers, 1986; Rogers, 1975, 1983).

We propose that awareness is in fact a multidimensional variable. That is, on one hand individuals need to be aware of threats associated with desktop security. On the other hand, the same individuals have to be aware

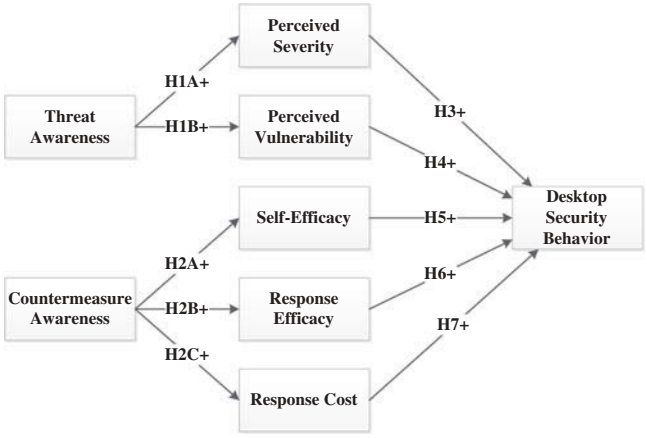

Figure 1. The research model.

of countermeasures that could be implemented against such threats. Our constructs of TA and CA are theoretically based on technology awareness introduced by Dinev and Hu (2007), who defined it as raised consciousness of and interest in knowing about technological issues and strategies to deal with them. In line with this, we define TA as user awareness of threats that can negatively affect his or her desktop security and CA as user awareness of countermeasures that can eliminate or minimize the risks associated with such threats. In this article, both TA and CA are operationalized through a construct introduced by Talib et al. (2010) to assess perceived understanding of the topics related to desktop security. These two types of awareness have different effects when applied within PMT settings. That is, knowledge about threats should result in more accurate estimates about the risks associated with them (i.e., the magnitude of their negative effects and the probability of being affected by them). A similar concept of threat probability of occurrence and its possible impact is also often used in risk assessment procedures associated with threat avoidance in organizational settings (Sumner, 2009), thus making it applicable in the context of our study. At the same time, if an individual is aware of possible countermeasures against such threats, he or she should be able to estimate whether it is possible to implement them in practice. Thus, TA has a positive effect on constructs in the threat appraisal process, i.e., PS, PV, while CA will positively influence those in the coping process, i.e., RE, SE, and RC. Therefore, we hypothesize the following:

H1a: TA will have a positive effect on PS.
H1b: TA will have a positive effect on PV.
H2a: CA will have a positive effect on SE.
H2b: CA will have a positive effect on RE.
H2c: CA will have a negative effect on RC.

DSB is the user actions that lead to the recommended security protection. Recommended behavior has been defined on the basis of literature available on this topic (CERT Coordination Center, 2002; Keller, Powell, Horstmann, Predmore, & Crawford, 2005). Behavior in the more general sense, following the definition provided by Merriam-Webster Online Dictionary (2010) can be thought of as a response of an individual to his or her environment. It is the ultimate goal for awareness and influenced by the above-mentioned constructs. Following Gurung et al. (2009), we have chosen to investigate the effects of threat and coping appraisals directly on behavior rather than on behavioral intentions, as the literature remains unclear about the interaction of intentions and cognitive variables in the PMT (Milne et al., 2000). Moreover, while the theoretical importance of intentions should not be underestimated, the ultimate goal in information security is protection from attackers. Therefore, the observation of end-user behaviors is more important, as it provides an objective measure of success of security training and education (Ng et al., 2009).

The threat appraisal process in the PMT involves three constructs. Our research model does not include the rewards construct as it would be conceptually difficult to distinguish between the value of risk behaviors and the cost of implementing preventive measure (i.e., there are no foreseeable benefits associated with avoiding recommended protective behaviors). Research also shows that the concept of rewards tends to be difficult to operationalize within various contexts (Abraham, Sheeran, Abrams, & Spears, 1994). Thus, we examine the other two constructs, PS and PV. PS conceptualizes how serious users believe that a potential threat may be (Milne et al., 2000), as well as the magnitude of the consequences of being affected by such threat (Gurung et al., 2009). PV refers to a user's assessment of whether he or she is susceptible to specific threats (Gurung et al., 2009; Milne et al., 2000). Empirical studies related to protective health behaviors (Armitage & Conner, 2001; Sutton, 1998) suggested that perceived level of risk and the likelihood of its occurrence are, in part, the determinants of risk-reduction behaviors (Ajzen, 2005; Becker, 1974; Maddux & Rogers, 1983). In general, greater levels of threat appraisal are associated with higher levels of fear that is caused by feelings of vulnerability to a threat and the seriousness of its consequences. Consequently, the greater the threat is, the more probable an individual is to be motivated to protect himself or herself (e.g., exercise recommended protective behaviour; Milne et al., 2000). Therefore, if users feel that the negative consequences of a given security threat are serious and likely to occur, they will be more motivated to execute recommended protective behaviors, thus mitigating the risks associated with such threats. On the other hand, if a threat is not serious then the risks associated with it could be accepted and no protective behavior would be implemented. Such approach is also in line with the phenomenon commonly known as risk management (Harris, 2008). Thus, both PS and PV reflect users' perceived risk related to occurrence of security threats and they have the potential of prompting user actions. We therefore propose the following hypotheses:

H3: PS affects users' DSB.

H4: PV affects users' DSB.

Coping appraisal, as defined earlier, includes three constructs: RE, SE, and RC. A good description of SE is provided by Ozer and Bandura (1990, p. 472), who defined it as "people's belief in their capabilities to mobilize the motivation, cognitive resources, and courses of action needed to exercise control over given events." The concept of SE has been initially conceived by Bandura (1977) and shown to be positively related to changes in behaviors (Bandura, Adams, Hardy, & Howells, 1980). Furthermore, Maddux and Rogers (1983) introduced SE within the ramifications of the PMT and demonstrated its usefulness as a determinant of behavioral intentions related to recommended protective behaviors. Consequently, if an individual believes that he or she can exercise such behaviors on his or her own, then it is more likely they will be enacted. On the other hand, if the recommended behaviors appear difficult to implement, a user may not engage in such activities, even though he or she may perceive the related threat to be serious. RE, in information security terms, is the extent to which a person believes that a particular action mitigates a security threat (Jayanti & Burns, 1998). In other words, RE can be defined as outcome expectations (Compeau & Higgins, 1995), since it is related to perceived consequences of certain behaviors (Venkatesh, Morris, Davis, & Davis, 2003). Compeau and Higgins (1995) found outcome expectations to be significant in predicting actual behavior. Therefore, if an individual perceives that a given security safeguard is easy to implement but expects the outcome of using such countermeasure to be ineffective, then he or she may not perform protective action anyway. Finally, RC is the third component of coping appraisal process. RC is related to the concerns about how costly it would be to perform recommended protective response (Milne et al., 2000). Such costs could include financial costs, time effort required to implement a protective safeguard, or cognitive effort associated with the protective behaviors. Thus, the following hypotheses are proposed:

H5: SE will have a positive relationship with recommended DSB.

H6: RE will have a positive relationship with recommended DSB.

H7: RC will have a positive relationship with recommended DSB.

Methodology

We collected data from a survey administered among undergraduate students in the business school at a large university in the southwestern United States. The participants included students enrolled in introductory management information systems (MIS) classes, as well as students enrolled in junior level MIS classes. The survey was administered over a 3-week period and provided a sample of 241 answers and yielded a response rate of almost 95%. Therefore, nonresponse bias is not an issue in this study. Twelve responses had to be discarded due to identical answers given to all questions.

The scales implemented in this study are based on previously validated ones. All items in the survey instrument were measured on a seven-point Likert scale. Questions referring to TA and CA asked for user familiarity with certain information security-related concepts from 1 = not familiar at All to 7 = very familiar. The questionnaire items for both TA and CA have been adapted from Talib et al. (2010). However, the scope of the items has been determined based on Ciampa (2010) in order to reflect topics specifically related to desktop security awareness area. Questions regarding PS, PV, RE, SE, RC, and DSB asked to express how much respondents agree with the respective statements in the questionnaire from 1 = strongly disagree to 7 = strongly agree. The survey instrument is described in detail in Table 1.

Data analysis and results

We analyzed the data using partial least squares (PLS) method with the help of SmartPLS software package (Ringle, Wende, & Will, 2005). We have chosen to analyze our data with PLS because our research model is focused on the predictive power of security awareness constructs (i.e., TA, CA) on human behavior. PLS-Structural Equation Modeling (SEM) is designed primarily for exploratory research by focusing on explaining the variance in the dependent variables when analyzing proposed theoretical models (Hair, Hult, Ringle, & Sarstedt, 2014). Since PLS emphasizes prediction over parameter accuracy, it is the preferred data analysis method for the context of our study (Gefen, Rigdon, & Straub, 2011). The results of theoretical model testing are presented in Figure 2.

Prior to the evaluation of the PLS model, we tested the sample data for heterogeneity and common method bias. The survey respondents were recruited from undergraduate business students. However, there

Table 1. Survey instrument.

Construct	Item	Item Text	Source
TA		On a scale from 1 to 7 (1 = not familiar at all; 7 = very familiar), please indicate your level of familiarity with the following terms:	Talib et al. (2010); Ciampa (2010)
	TA1	Virus	
	TA2	Worm	
	TA3	Trojan horse	
CA	CA1	Installation of operating system updates	
	CA2	Antivirus software	
	CA3	Firewall	
	CA4	Data backup	
PS	PS1	I believe that having my computer infected by a virus would be a severe problem	Crossler (2010); Witte et al. (1996)
	PS2	I believe that having my computer infected by a virus is a serious problem	
	PS3	I believe that having my computer infected by a virus is a significant problem	
	PS4	I believe that having my computer infected by a worm would be a severe problem	
	PS5	I believe that having my computer infected by a worm is a serious problem	
	PS6	I believe that having my computer infected by a worm is a significant problem	
PV	PV1	I am at risk of having a Trojan horse installed on my computer	
	PV2	It is likely that I will have a Trojan horse installed on my computer	
	PV3	It is possible that I will have a Trojan horse installed on my computer	
	PV4	I am at risk of having my computer infected with a virus	
	PV5	It is likely that I will have my computer infected with a virus	
	PV6	It is possible that I will have my computer infected with a virus	
SE	SE1	I am able to set up antivirus software on my computer to prevent virus infections on my system	
	SE2	I am able to apply security updates to my operating system	
	SE3	Installing firewall software is a convenient way of blocking unauthorized access to my computer	
	SE4	I believe I can configure my computer to provide good protection from software attacks	
RE	RE1	Installation and frequent updates of antivirus software is effective in preventing virus infections on my computer	
	RE2	If I install antivirus software on my computer and update it frequently, I am less likely to have my system infected by a virus	
	RE3	Installation and configuration of firewall software on my computer is effective in preventing unwanted traffic on my computer	
	RE4	Applying security patches on my operating system is an effective way of preventing hacker attacks on my computer	
RC	RC1	Installation of antivirus software requires significant financial cost	
	RC2	Updating antivirus software requires significant financial cost	
	RC3	Updating my operating system requires significant financial cost	
	RC4	Checking my computer for suspicious activity requires significant financial cost	
	RC5	Installation of firewall requires significant financial cost	
DSB	DSB1	I have antivirus software installed on my computer	CERT Coordination Center (2002); Keller et al. (2005)
	DSB2	I have antivirus software frequently updated in order to protect my computer from attacks	
	DSB3	I have my operating system frequently updated in order to protect my computer from attacks	
	DSB4	I periodically check my computer for suspicious activity	
	DSB5	I have firewall installed and enabled on my computer	

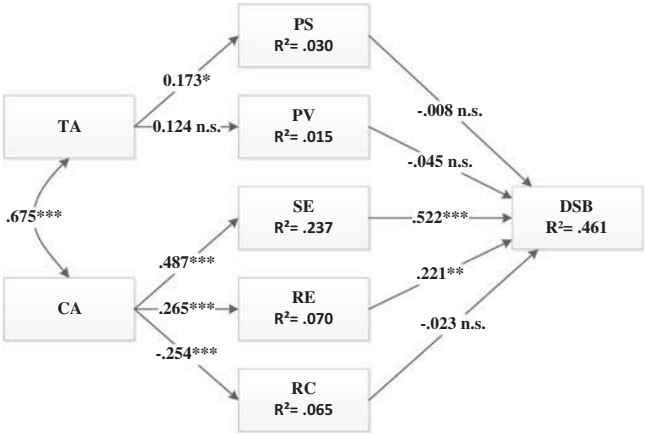

Figure 2. Research model results (***$p < 0.001$; **$p < 0.01$; *$p < 0.05$; n.s.—not significant).

were no significant differences observed between males and females (140 versus 89), as well as between different majors (e.g., accounting, marketing, management, information systems, etc.). In addition, the respondents were asked to report the major operating systems running on their personal computers, and to disclose whether they have been previously affected by any type of malware (e.g., virus, worm, Trojan, etc.). The majority of the respondents (183) indicated Microsoft (MS) Windows as their primary operating system, followed by OS X (44). Only two students used Linux (any distribution) as their primary environment. As for malware infection, 116 respondents had their PCs previously infected by malicious software. However, no significant differences existed between the two groups when evaluating the research model. Therefore, we concluded that the sample employed in the study is homogenous.

With regards to common method bias, we performed Harman's single factor test to verify whether one factor accounted for the majority of variance in our data. We conducted an exploratory factor analysis on

all items without rotation. The results yielded 37 factors, the largest of which accounted for approximately 26% of variance, thus showing no evidence of common method bias. However, Harman's test should rather be treated as diagnostic than a remedy (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Therefore, we also verified that no two latent variable correlations are higher than 0.90 (Table 3), which could be another indication of common method bias (Vance et al., 2012). Finally, following Podsakoff et al. (2003) and Liang, Saraf, Hu, and Xue (2007), we included a common method factor whose indicators included measurement items and for each indicator calculated the portion of its variance that was explained by the construct and method, respectively. The results showed that the variance substantively explained by the underlying construct was on average 0.77, whereas the average method-based variance was 0.006 (the ratio of substantive variance to method variance is approximately 126:1). Therefore, we have concluded common method bias is unlikely to be a concern in this study.

Evaluation of the PLS model is a two-step process. First, the outer model needs to be assessed, which is followed by the evaluation of the inner model. Evaluation of PLS estimates provides information about a measurement's reliability and validity. It is only possible to make inferences from the inner model once the outer model has been confirmed for reliability and validity (Henseler, Ringle, & Sinkovics, 2009). All constructs employed in the study are operationalized as reflective. The summary of reliability and validity analysis is presented in Tables 2 and 3. Reliability of the research model is checked through Cronbach's alpha and composite reliability. The difference between these two criteria is that Cronbach's alpha assumes the equal reliability of all indicators, whereas in PLS items are prioritized on their reliability, which provides a more reliable composite. Furthermore, it is believed that Cronbach's alpha is likely to underestimate the internal consistency reliability of latent variables in PLS models. Therefore, it is advised to rely on composite reliability (Werts, Linn, & Jöreskog, 1974). In this research, no matter which of the two criteria mentioned above is used, all values are above the recommended 0.7 (Henseler et al., 2009).

Convergent validity, the extent to which a measure correlates with alternative measures of the same construct (Hair, Hult, Ringle, & Sarstedt, 2014), can be

Table 2. Measurement item cross loadings to latent constructs.

Item	TA	CA	DSB	PS	PV	RC	RE	SE	*t* Statistic	*p*-Value	VIF
TA1	0.91	0.66	0.21	0.22	−0.09	−0.14	0.18	0.33	10.22	<0.001	1.908
TA2	0.82	0.56	0.22	0.00	−0.12	−0.14	0.12	0.28	6.50	<0.001	2.447
TA3	0.90	0.61	0.28	0.13	−0.13	−0.17	0.14	0.34	10.42	<0.001	2.596
CA1	0.47	0.75	0.23	0.08	−0.15	−0.25	0.18	0.38	64.35	<0.001	1.532
CA2	0.66	0.92	0.35	0.12	−0.16	−0.22	0.29	0.49	22.88	<0.001	3.894
CA3	0.68	0.92	0.38	0.11	−0.18	−0.18	0.23	0.44	16.28	<0.001	4.408
CA4	0.58	0.82	0.33	0.13	−0.18	−0.22	0.20	0.33	69.59	<0.001	2.189
DSB1	0.14	0.22	0.85	0.16	−0.10	−0.09	0.46	0.49	28.87	<0.001	5.011
DSB2	0.16	0.21	0.86	0.12	−0.11	−0.10	0.45	0.47	32.00	<0.001	5.196
DSB3	0.23	0.33	0.81	0.14	−0.22	−0.23	0.40	0.55	20.28	<0.001	1.921
DSB4	0.31	0.42	0.74	0.18	−0.07	−0.19	0.31	0.59	17.08	<0.001	1.589
DSB5	0.23	0.35	0.82	0.23	−0.08	−0.17	0.43	0.55	22.42	<0.001	2.045
PS1	0.15	0.13	0.24	0.90	−0.07	−0.01	0.33	0.27	43.72	<0.001	6.643
PS2	0.19	0.15	0.18	0.93	−0.08	−0.04	0.34	0.21	52.54	<0.001	10.732
PS3	0.18	0.14	0.20	0.89	−0.03	−0.03	0.32	0.24	29.63	<0.001	9.372
PS4	0.13	0.08	0.16	0.91	−0.06	−0.04	0.32	0.21	38.74	<0.001	11.838
PS5	0.14	0.09	0.16	0.92	−0.07	−0.09	0.31	0.22	38.00	<0.001	19.898
PS6	0.13	0.09	0.17	0.87	−0.04	−0.08	0.28	0.20	25.04	<0.001	11.581
PV1	−0.09	−0.17	−0.11	−0.07	0.88	0.33	−0.05	−0.12	11.32	<0.001	4.196
PV2	−0.10	−0.19	−0.13	−0.10	0.89	0.34	−0.04	−0.12	11.88	<0.001	5.121
PV3	−0.02	−0.13	−0.08	−0.06	0.85	0.22	−0.03	−0.12	9.56	<0.001	4.859
PV4	−0.14	−0.17	−0.13	−0.04	0.90	0.28	−0.02	−0.14	13.09	<0.001	4.113
PV5	−0.16	−0.23	−0.17	−0.06	0.93	0.38	−0.04	−0.19	14.30	<0.001	5.229
PV6	−0.06	−0.08	−0.08	−0.02	0.86	0.19	0.04	−0.10	10.99	<0.001	4.795
RC1	−0.14	−0.15	−0.11	−0.01	0.32	0.79	−0.03	−0.11	17.99	<0.001	2.106
RC2	−0.18	−0.25	−0.18	−0.08	0.34	0.91	−0.16	−0.22	51.82	<0.001	3.498
RC3	−0.08	−0.14	−0.10	−0.03	0.26	0.82	−0.07	−0.10	35.75	<0.001	2.436
RC4	−0.17	−0.27	−0.22	−0.05	0.29	0.89	−0.21	−0.28	56.05	<0.001	2.822
RC5	−0.14	−0.22	−0.17	−0.02	0.29	0.87	−0.10	−0.23	21.21	<0.001	2.646
RE1	0.13	0.24	0.51	0.30	−0.05	−0.14	0.94	0.50	90.92	<0.001	5.699
RE2	0.10	0.23	0.46	0.29	−0.05	−0.14	0.94	0.50	79.36	<0.001	5.843
RE3	0.22	0.25	0.45	0.35	−0.01	−0.14	0.91	0.48	48.59	<0.001	3.419
RE4	0.18	0.27	0.45	0.36	0.00	−0.14	0.91	0.51	38.57	<0.001	3.389
SE1	0.36	0.42	0.59	0.29	−0.14	−0.23	0.53	0.88	32.56	<0.001	2.910
SE2	0.35	0.49	0.59	0.25	−0.18	−0.27	0.49	0.91	54.93	<0.001	3.361
SE3	0.19	0.32	0.54	0.19	−0.06	−0.15	0.45	0.84	26.36	<0.001	2.279
SE4	0.35	0.45	0.55	0.15	−0.16	−0.17	0.39	0.85	33.08	<0.001	2.163

VIF: variance inflation factor.

Table 3. Construct correlations, AVE, and construct reliabilities.

Construct	CR	R^2	α	AVE	TA	CA	DSB	PS	PV	RC	RE	SE
TA	0.91	0.00	0.86	0.77	0.88							
CA	0.92	0.00	0.87	0.73	0.70	0.85						
DSB	0.91	0.46	0.87	0.67	0.26	0.38	0.82					
PS	0.96	0.03	0.96	0.82	0.17	0.13	0.21	0.91				
PV	0.96	0.02	0.95	0.78	−0.12	−0.20	−0.14	−0.06	0.89			
RC	0.93	0.06	0.91	0.73	−0.17	−0.25	−0.20	−0.05	0.35	0.86		
RE	0.96	0.07	0.94	0.86	0.17	0.27	0.50	0.35	−0.03	−0.15	0.93	
SE	0.93	0.24	0.89	0.76	0.36	0.49	0.65	0.25	−0.16	−0.24	0.54	0.87

examined either through investigation of outer loadings of indicators, as well as the average variance extracted (AVE). The former criterion assumes that outer loadings on a construct should be at least 0.708 or higher. All measurement items used in this study meet this criterion (Table 2). On a construct level, AVE is a common measure of convergent validity. Minimum acceptable threshold is 0.5 or more, which indicates that construct explains more than half of the variance in its indicator items. In this study, all construct have their respective AVE values exceeding this threshold (with DSB being the lowest at 0.67), thus indicating sufficient convergent validity (Table 3).

Following current literature (Gefen & Straub, 2005; Hair, Hult, Ringle, & Sarstedt, 2014), discriminant validity has been established using two criteria. First, it has been evaluated by examining measurement item cross loadings. According to this criterion discriminant validity is achieved when each indicator outer loadings on the associated construct is higher than its cross loadings on other constructs. All indicators included in our study have their outer loadings on intended constructs higher than any of their cross loadings on other constructs. The Fornell–Larcker criterion is the second measure used to check for discriminant validity (Fornell & Larcker, 1981). When applied to PLS method, as a rule of thumb, the square root of AVE from each latent variable is supposed to be higher than the correlations with all other latent variables. Latent variable correlations matrix is presented in Table 3. DSB has the lowest AVE of 0.67 (square root of which is equal to 0.82). Therefore, discriminant validity is confirmed. Having established reliability and validity of the model, it is possible to evaluate the inner path model estimates. According to Henseler et al. (2009), the individual path coefficients in the PLS structural model can be interpreted as standardized beta coefficients of OLS regressions. Also, in order to obtain the confidence intervals of the path coefficients and statistical inference, bootstrapping technique was used. Per recommendation of Hair, Hult, Ringle, & Sarstedt (2014), the number of bootstrap samples has been set to 5000. The final results are presented in Table 4. In summary, all of the hypotheses in our model, except H1b, H3, H4, and H7, are supported.

Table 4. Overview of structural model findings.

Hypothesis	Path Coefficient	Standard Error	*t* Statistic	Supported?
H1a: TA → PS	0.173	0.089	1.960	Supported
H1b: TA → PV	−0.124	0.076	1.628	Not supported
H2a: CA → RC	−0.254	0.053	4.863	Supported
H2b: CA → RE	0.265	0.073	3.646	Supported
H2c: CA → SE	0.487	0.065	7.515	Supported
H3: PS → DSB	−0.008	0.060	0.129	Not supported
H4: PV → DSB	−0.045	0.058	0.777	Not supported
H5: SE → DSB	0.522	0.077	6.744	Supported
H6: RE → DSB	0.221	0.085	2.595	Supported
H7: RC → DSB	−0.023	0.062	0.377	Not supported

Discussion

The overall R^2 is 0.461; that is, our model explains 46.1% of the variance in DSB. As a rule of thumb, this value can be described as moderate given the exploratory nature of our study (Chin, 1998; Hair, Hult, Ringle, & Sarstedt, 2014) and is within well-accepted standards for behavioral research (Keith, 2005; Kenny, 1979). In addition, we have conducted a post hoc power analysis using G*Power software package (Faul, Erdfelder, Buchner, Lang, 2009). The number of exogenous variables (7) and the sample size (241) were used as the baseline. Given the input, the results indicate that the statistical power of this study is above 0.99 (exceeding the recommended threshold of 0.80) for moderate and large effect size, thus showing that our sample size was large enough to test all the hypotheses in the research model. Our findings indicate that TA is a significant determinant of PS but not PV (H1a is supported but H1b is not). One possible explanation is that home users are more exposed to information about the negative consequences of information security threats, but they lack expertise in assessing the risks of being affected by such threats. It is likely individuals may often fall victim of software vendors' marketing efforts, which could inflate the perception of threats. In the meantime, such marketing efforts often downplay the importance of risk

assessment of individual cases. Instead, they try to instill the belief that, if users install (and consequently subscribe to a particular vendor's product, they will not be exposed to security threats.

Our results also indicate that awareness of countermeasures is a critical determinant of coping appraisal mechanisms (H2a, H2b, and H2c supported). Therefore, it is simply not enough to be aware of threats, if an individual is not able to identify tools or techniques that could help his or her implement protection. Only when users are aware of such countermeasures, can they assess their abilities to use them effectively. Since our study reflects relatively well known issues in security, the results indicate that the participants are aware of countermeasures against desktop security threats and they seem fairly confident about using them (significant relationship between CA and SE, i.e., H2a). They also believe in the relative effectiveness of the presented countermeasures (significant relationship between CA and RE, i.e., H2b). In addition, users who are more aware of the countermeasures are also more likely to perceive RC to be lower than users whose CA is low (significant negative relationship between CA and RC, i.e., H3).

The results do not provide support for H3 and H4, which posit that threat appraisal has significant effect on behavior. While this finding is against theoretical propositions of the PMT, previous PMT research has repeatedly shown that threat appraisal is a poor predictor of both behavioral intentions and behaviors (Abraham et al., 1994; Hodgkins & Orbell, 1998; Maddux & Rogers, 1983). One possible explanation is that a moderator variable that is influencing behavior may exist. However, PMT-related research has not identified any theoretically important variable that would not be context dependent (Witte & Allen, 2000). Another possible explanation is that very often both positive and negative associations between risk and behaviors can be observed. For example, if a user perceives himself or herself as vulnerable to a given threat, then he or she may actually enact the protective behavior. On the other hand, if such behavior has been already implemented, then the user may no longer feel threatened, which would lead to a negative association between PV and behavior. The lack of significance could also indicate that our sample was not homogenous, i.e., it combined more experienced users with less experienced ones as well (meaning that both positive and negative relationships between the two variables exist in our data (Milne et al., 2000). Another common issue with the measurement of PV that it is often viewed as a static variable and often measured in isolation is whether individuals are actually aware of a threat or not (Weinstein, 1988). Our study addresses this issue by introducing TA as an antecedent of PV. While the relationship between the two is not significant, this lack of significance can be attributed to heterogeneity of participants in our sample. That is, some of them may only be aware of the existence of desktop security threats, while others may be actually aware of how dangerous a threat is and thus attribute the risk of being affected by them. Thus the lack of significance between TA and PV, and between PV and DSB is observed within the context of our study. The lack of significant correlation between PS and DSB, while unexpected, can be explained through potential multidimensionality of PS. Several studies on the PMT suggest that difficulty in obtaining variability in the data for PS measurement is another potential reason for lack of significance for severity (Harrison, Mullen, & Green, 1992). It is possible that the effects of threat appraisal variables on behavioral intentions or behaviors are mediated by other components of the PMT (Johnston & Warkentin, 2010; Milne et al., 2000; Witte et al., 1996) or that there are other relevant factors not captured by our research model. Overall, lack of support of our hypotheses in this respect is consistent with what have been reported in prior PMT studies.

As for the coping appraisal our results support the claims that SE and RE are significant determinants of protective behavior (support for H5 and H6). Our findings are in line with previous research, where SE and RE are the most stable predictors of protective behaviors (Crossler, 2010; Gurung et al., 2009; Vance et al., 2012; Woon et al., 2005). At the same time, RC did not significantly affect protective DSBs. Therefore, it appears that home users are not only aware of desktop security threat countermeasures (support for H2a, H2b, and H2c), but they are also comfortable with using them (support for H5 and H6). However, the cost of implementing these countermeasures is not found to affect users' protective behaviors (H7 not supported). One possible explanation is that such countermeasures are available to the public for little or no cost. For example, firewall and data backup solutions are usually built-in features of an operating system, and can be quickly accessed and set up with little effort. Antivirus and antispyware software is also often available for free, while paid subscription services are often bundled with the purchase of new hardware. Overall, such tools can be easily obtained by the general public, and their user interface is designed for casual users, so that protective services can be easily started. Our results indicate that home users do not perceive RC to be a

significant obstacle preventing them from implementing protective DSBs.

In addition to our initial research model, we have also tested for the correlation between TA and CA. Pearson's r is 0.675 and is significant at 0.001 level. The results reveal that even though the constructs are highly correlated, their correlation levels are within an acceptable threshold per Fornell-Larcker criterion (see Table 3). What is more interesting is that users who are aware of threats are also more aware of their respective countermeasures. Consequently, it appears that effective security training and education programs should take a systematic approach by making sure that they address multiple dimensions of security awareness. That is, individuals should be educated both about the risks associated with threats and about the respective countermeasures that could be employed to either avoid threats, or minimize the risks associated with them. However, implementing such a structured training approach is more feasible in organizational settings, where the content, the delivery methods, and the evaluation of results depend to a large extent on the organization's IT management. This is in stark contrast to the context of individual users, who have total control. Thus, home users cannot individually be part of such "methodology" and are often left with acquiring training on their own as the only alternative. Also, there is a risk that home users will become aware of the threats only after they have experienced the negative effects of security threats, and after damage has already been done. Nevertheless, our data analysis did not find significant differences in terms of DSB between those affected by malware and those who were not. We conclude that individual users often rely on third parties (e.g., word-of-mouth, security vendor web sites, user forums, discussion groups, and social media) to increase their levels of security awareness. Such an approach cannot be considered a highly effective one. For example, all major web browsers warn users of phishing attempts. At the same time, research shows that such warnings do not work as expected unless they are extremely easy to use (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). Furthermore, previous research shows that for home users, the majority of the learning about information security occurs at the workplace (Talib et al., 2010), thus making it even more difficult to design effective training for home users. It does appear though, that if society at large emphasizes the importance of information security, users will be more proactive in educating themselves. Some additional responsibility could also be placed on security vendors and authorities to provide a more proactive learning approach for home users once they start using certain protective technologies (Woon et al., 2005). At this point, however, building awareness among individual users to a large extent relies on transference of knowledge from organizations and skills acquired at educational institutions.

Implications and limitations

The goal of this study is to determine whether desktop security awareness (represented by TA and CA) influences DSBs from the PMT perspective. We found that TA impacts users' perception of severity, but not that of vulnerability, and that CA impacts the elements of coping appraisal processes. Our study also indicates that RE and SE are important predictors of DSB.

As a main contribution, this study extends the current body of knowledge by introducing the concept of awareness as a significant predictor of coping and threat appraisal processes. Whereas prior studies predominantly focus on the constructs and process endogenous to the PMT, we examine the roles played by an important antecedent to those constructs and processes. Thus, this study paints a fuller picture of how home users deal with desktop security.

This study also highlights that awareness should be thought of as a multidimensional concept by itself. It demonstrates that the two different dimensions of awareness, that of threats and that of countermeasures, have different influences on users' behaviors. Overall, CA seems to be a more powerful predictor of behaviors, its effect mediated by efficacy beliefs. This suggests that, when conducting awareness education, it is not sufficient to create the "fear appeal" (Johnston & Warkentin, 2010) in the hope of motivating users to act. Users are more likely to be motivated if they are aware of protective measures and are confident to use them. That said, the roles of TA deserve scrutiny of future studies. As mentioned above, its lack of significant effect on PV could be due to the limitations of this study; and the non-significant relationships between threat appraisal constructs (PS and PV) and behavior are not atypical of PMT research.

Our conceptualization of awareness also sheds light on PS and PV as frequently unstable predictors of recommended security behaviors, indicating that the former can actually be a multidimensional concept, while the latter should be approached as a dynamic rather than static variable. Future studies may investigate this aspect for more insights. This study is one of the first to integrate an important antecedent to the threat appraisal and coping appraisal processes in the

PMT. It shows the promise of additional explanation power that can be generated by so doing.

From the practical perspective, our study reveals that effective information security awareness and training programs (i.e., those that lead to improvement in exercising protective behaviors) should reflect the concept of multidimensionality of awareness, as it is not enough to educate individuals about threats but their respective countermeasures, and vice versa. Furthermore, it appears that such programs should also pay more attention to educating users about assessing the risks caused by the threats, especially if the marketing efforts of security vendors are taken into consideration, as they may skew users' perception of information security. In summary, this study offers several important insights. It shows that security awareness education is not necessarily about designing different content for different audiences, but more about assuring that security awareness activities address each dimension of awareness in a comprehensive manner. For example, it is not enough to know how to recognize threats and risks associated with them, if users do not know how to avoid them. Similarly, knowledge of countermeasures is of little to no use, if users do not know how to recognize threats and evaluate their respective risks. The different dimensions of security awareness determine the formation of different elements of protection motivation. Consequently, each of the dimensions needs to receive attention, so that the users can receive comprehensive information allowing them to effectively avoid security threats in the future.

The fact that this study was conducted on a sample composed only by undergraduate college students may limit the ability to extrapolate results of this study towards more general population. College students may have different levels of computer literacy than other groups in the society. On the other hand, it is widely known that young people tend to act more emotionally than rationally. As mentioned above, we suspect that some differences within the students in our sample (e.g., some of them had more exposure to security information due to the additional coursework they have taken) was a reason for some of the non-significant relationships in the model. Finally, this research was only limited to desktop security, which is a small (albeit important) fraction of information security. Future studies should address whether our findings can be generalized to other people or settings. The present study represents a compromise between the degree of generalizability and the resource availability (Shadish, Cook, & Campbell, 2002). Other areas should also be studied to determine whether PMT is appropriate for evaluating other information security behaviors.

Another potential limitation of this study is the conceptualization of RC. We have focused solely on the financial aspect of the construct, although traditionally it also includes time and cognitive effort as other costs related to exercising recommended protective behaviors. At present, most of consumer-oriented security software (e.g., antivirus, firewall, software updates, backup solutions, etc.) requires relatively little attention from a user during setup and initial configuration and usually runs in an unobtrusive and automated manner delivering "one size fits all" protection. At the same time, such protective software usually provides power users with access to more advanced configuration options. However, our study was not focused on investigating the differences between different types of users. In addition, the survey participants were recruited from undergraduate students in a business school. As such, they may not necessarily have the required technical skills to go beyond the typical recommended settings provided to them by the security vendors. In contrast, time and cognitive effort would play a significant role if the study had been executed among information security professionals, whose responsibility is to deliver a safe computing platform to other members of their respective organizations. Future research should address this potential issue. Another worthy subject of future studies is knowledge transference between work and home settings. For example, researchers may examine the magnitude of the effect of organizational training programs on exercising recommended security behaviors at home. Since our sample consisted primarily of undergraduate college students with little to no professional experience, we were unable to compare laypeople with professionals or to examine the effect of different sources of information in implementing protective behaviors. These can be achieved in future studies. From theoretical perspective, they would be in line with the extended version of PMT (Milne et al., 2000; Rogers, 1983).

This study conceptualizes desktop security awareness in terms of major dimensions—countermeasure and TA. These constructs are introduced as antecedents of the elements of coping and threat appraisals, respectively. Since the two dimensions of desktop security awareness were tested through the theoretical lens of a mature theory, it was necessary to examine the effects of each on the elements of PMT. As a result, the research model and its subsequent hypotheses represent a compromise between

model comprehensiveness and parsimony. Such a design, while ensuring the academic rigor of the study, may unfortunately result in less straightforward interpretation of practical implications. On the other hand, to ensure that our research model covers the entire gamut of the phenomenon under study, we chose to avoid a reduction in the number of hypotheses. This helped to avoid the common risk of underspecification of research models (Bacharach, 1989). At the same time, a post hoc power analysis revealed that our sample size was large enough to support all the hypotheses.

Conclusion

With the proliferation of the Internet and mobile technologies, information security awareness of home users is an important factor for the global community. Yet the area of desktop security still remains a significant concern for modern society. Our study offers in-depth insights into home user information security awareness. It investigates the phenomenon based on the framework of the PMT and extends current body of knowledge by introducing security awareness as an antecedent of protective behaviors mediated by coping and threat appraisals. Our results provide strong support for the proposed theoretical model, and emphasize the multidimensional nature of security awareness. Therefore, promoting the best practices of information security awareness among home users should reflect the complex nature of the awareness building processes, thus assuring such individuals are provided with a complete perspective of the phenomenon.

Notes on contributors

Bartlomiej Hanus is an assistant professor in the School of Business at Emporia State University. He received a PhD in Business Computer Information Systems from the University of North Texas. He also holds an MS in Information Technologies from University of North Texas. His research interests include information security, cloud computing, data analytics (with focus on web mining), and decision making under stress.

Yu "Andy" Wu is an associate professor in the Department of Information Technology and Decision Sciences, College of Business at the University of North Texas. He received a PhD (2007) and an MS (2003) in MIS from the University of Central Florida, Orlando, FL. Andy's primary research interests include information security and social networks. His articles appeared in journals such as *IEEE Transactions on Professional Communication, Informing Science, Journal of Organizational and End User Computing, Information Resource Management Journal*, and the proceedings of a number of international conferences. Before his academic career, Andy had 7 years of experiences in various technical and business positions.

References

Abraham, C. S., Sheeran, P., Abrams, D., & Spears, R. (1994). Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of HIV infection. *Psychology & Health*, *9*(4), 253–272. doi:10.1080/08870449408407485

Ajzen, I. (2005). *Attitudes, personality and behavior* (2nd ed.). Maidenhead, UK: Open University Press.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432–445. doi:10.1016/j.cose.2009.12.005

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), A613–A615.

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology*, *40*(4), 471–499. doi:10.1348/014466601164939

Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. *Academy of Management Review*, *14*(4), 496–515.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. doi:10.1037/0033-295X.84.2.191

Bandura, A., Adams, N. E., Hardy, A. B., & Howells, G. N. (1980). Tests of the generality of self efficacy theory. *Cognitive Therapy and Research*, *4*(1), 39–66. doi:10.1007/BF01173354

Becker, M. H. (1974). The health belief model and sick role behavior. *Health Education Monographs*, *2*, 409–419.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164. doi:10.1057/ejis.2009.8

CERT Coordination Center. (2002). *Home computer security*. Retrieved from http://www.cert.org/homeusers/HomeComputerSecurity/

Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In G. A. Marcoulides (Ed.), Modern methods for Business Research (pp. 295–358). Mahwah, NJ: Lawrence Erlbaum Associates.

Ciampa, M. (2010). *Security awareness: Applying practical security in your world* (3rd ed.). Boston, MA: Course Technology.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189–211. doi:10.2307/249688

Crossler, R. E. (2010, January). *Protection motivation theory: Understanding determinants to backing up personal data*. Paper presented at the 43rd Hawaii International Conference on System Sciences, Honolulu, HI.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153. doi:10.1046/j.1365-2575.2001.00099.x

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), 386–408.

Dunlop, C., & Kling, R. (1992). Social relationships in electronic commerce—introduction. In C. Dunlop & R. Kling (Eds.), *Computerization and controversy—value conflicts and social change*. San Diego, CA: Academic Press.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*, 1149–1160. doi:10.3758/BRM.41.4.1149

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research (JMR)*, *18*(3), 382–388. doi:10.2307/3150980

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

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(1), 109.

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management & Computer Security*, *17*(3), 276–289. doi:10.1108/09685220910978112

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage.

Harris, S. (2008). *CISSP all-in-one exam guide* (4th ed.). New York, NY: McGraw-Hill.

Harrison, J. A., Mullen, P. D., & Green, L. W. (1992). A meta-analysis of studies of the health belief model with adults. *Health Education Research*, *7*(1), 107–116. doi:10.1093/her/7.1.107

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing (AIM)*, *20*, 277–320.

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. doi:10.1057/ejis.2009.6

Herold, R. (2010). *Managing an information security and privacy awareness and training program*. Boca Raton, FL: CRC Press.

Hinde, S. (2001). The weakest link. *Computers & Security*, *20*(4), 295–301. doi:10.1016/S0167-4048(01)00403-5

Hodgkins, S., & Orbell, S. (1998). Can protection motivation theory predict behaviour? A longitudinal test exploring the role of previous behaviour. *Psychology & Health*, *13*(2), 237–250. doi:10.1080/08870449808406749

James, T., Nottingham, Q., & Kim, B. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information Technology and Management*, *14*(2), 69–89. doi:10.1007/s10799-012-0147-4

Jayanti, R. K., & Burns, A. C. (1998). The antecedents of preventive health care behavior: An empirical study. *Journal of the Academy of Marketing Science*, *26*(1), 6–15. doi:10.1177/0092070398261002

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–A544.

Keith, T. Z. (2005). *Multiple regression and beyond*. Boston, MA: Pearson.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management*, *22*(2), 7–19. doi:10.1201/1078/45099.22.2.20050301/87273.2

Kenny, D. A. (1979). *Correlation and causality*. New York, NY: Wiley.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847. doi:10.1016/j.cose.2010.08.001

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, *46*(1), 254–264. doi:10.1016/j.dss.2008.06.010

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 1–31. doi:10.1145/1754393

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communicable ACM*, *51*(3), 71–76. doi:10.1145/1325555

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, *31*(1), 59–87.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. doi:10.1016/0022-1031(83)90023-9

McAfee Labs. (2010). *McAfee Threats report: Third quarter 2010*. Retrieved from http://www.mcafee.com/us/local_content/reports/q32010_threats_report_en.pdf

Merriam-Webster Online Dictionary. (2010). *Behaviour*. Retrieved from http://www.merriam-webster.com/dictionary/behavior

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143. doi:10.1111/jasp.2000.30.issue-1

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. doi:10.1016/j.dss.2008.11.010

Ozer, E. M., & Bandura, A. (1990). Mechanisms governing empowerment effects: A self-efficacy analysis. *Journal of*

Personality and Social Psychology, *58*(3), 472–486. doi:10.1037/0022-3514.58.3.472

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). *Employees' behavior towards is security policy compliance*. Paper presented at the 40th Annual Hawaii International Conference on System Sciences, Waikoloa, HI.

Parsons, T. (1991). *The social system* (2nd ed.). London, UK: Routledge.

Peltier, T. (2000). Security awareness program. In H. F. Tipton & M. Krause (Eds.), *Information security management*. Boca Raton, FL: Auerbach Publications.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, *88*(5), 879–903. doi:10.1037/0021-9010.88.5.879

Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research*, *1*(3), 153–161. doi:10.1093/her/1.3.153

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 767–A764.

Ringle, C. M., Wende, S., & Will, A. (2005). *SmartPLS 2.0*. Retrieved from www.smartpls.de

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. doi:10.1080/00223980.1975.9915803

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

Rosenstock, I. M. (1966). Why people use health services. *The Milbank Memorial Fund Quarterly*, *44*(3), 94–127. doi:10.2307/3348967

SANS Institute. (2010). *The top cyber security risks*. Retrieved from http://www.sans.org/top-cyber-security-risks/

Senge, P. M. (1994). *The fifth discipline: The art & practice of the learning organization*. New York: Currency Doubleday.

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

Shimeall, T. (2002). *Cyberterrorism*. Retrieved from http://www.cert.org/homeusers/HomeComputerSecurity/

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. doi:10.1108/09685220010371394

Siponen, M. (2001). Five Dimensions of Information Security Awareness. *Computers & Society*, *31*(2), 24–29.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469. doi:10.2307/249551

Sumner, M. (2009). Information security threats: A comparative analysis of impact, probability, and preparedness. *Information Systems Management*, *26*(1), 2–12. doi:10.1080/10580530802384639

Sutton, S. (1998). Predicting and explaining intentions and behavior: How well are we doing? *Journal of Applied Social Psychology*, *28*(15), 1317–1338. doi:10.1111/jasp.1998.28.issue-15

Symantec. (2010). *Norton cybercrime report: The human impact*. Retrieved from www.norton.com/cybercrimereport

Symantec. (2012). *Norton cybercrime report 2012*. Retrieved from http://us.norton.com/cybercrimereport

Talib, S., Clarke, N. L., & Furnell, S. (2010, February). *An analysis of information security awareness within home and work environments*. Paper presented at the International Conference on Availability, Reliability, and Security (ARES'10), Krakow, Poland.

Thomson, M. E., & Von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173. doi:10.1108/09685229810227649

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198. doi:10.1016/j.im.2012.04.002

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478.

Warkentin, M., Malimage, N., & Malimage, K. (2012, December). *Impact of protection motivation and deterrence on IS security policy compliance: A multi-cultural view* (Paper 20). Paper presented at the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC), Orlando, FL.

Weinstein, N. D. (1988). The precaution adoption process. *Health Psychology*, *7*(4), 355–386. doi:10.1037/0278-6133.7.4.355

Weinstein, N. D. (1993). Testing four competing theories of health-protective behavior. *Health Psychology*, *12*(4), 324–333. doi:10.1037/0278-6133.12.4.324

Werts, C. E., Linn, R. L., & Jöreskog, K. G. (1974). Intraclass reliability estimates: Testing structural assumptions. *Educational and Psychological Measurement*, *34*(1), 25–33. doi:10.1177/001316447403400104

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, *27*(5), 591–615. doi:10.1177/109019810002700506

Witte, K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), 317–342. doi:10.1080/108107396127988

Woon, I., Tan, G.-W., & Low, R. (2005, December). *A protection motivation theory approach to home wireless security*. Paper presented at the Proceedings of the 26th International Conference on Information Systems, Las Vegas, NV.