The Data Base for Advances in Information Systems

Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future

Steffi Haag
Friedrich-Alexander University Erlangen-Nürnberg

Mikko Siponen
University of Jyväskylä

Fufan Liu
University of Jyväskylä

Date of Acceptance: 3/6/2020

Please cite this article as follows:
Haag, S., Siponen, M., Liu, F. (Forthcoming). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *The Data Base for Advances in Information Systems*, In Press.

Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future

Steffi Haag
Friedrich-Alexander University Erlangen-Nürnberg

Mikko Siponen
University of Jyväskylä

Fufan Liu
University of Jyväskylä

Acknowledgments

We thank the senior editor, Tom Stafford, and the review team for their commitment and comments during the review process.

Abstract

Protection motivation theory (PMT) is one of the most commonly used theories to examine information security behaviors. Our systematic review of the application of PMT in information systems (IS) security and the comparison with its application for decades in psychology identified five categories of important issues that have not yet been examined in IS security research. Discussing these issues in terms of why they are relevant and important for IS security, and to what extent IS research has not considered them, offers new research opportunities associated with the study of PMT and IS security threats. We suggest how future studies can approach each of the open issues to provide a new road map for quantitative and qualitative IS scholars.

Keywords: Protection Motivation Theory; Behavioral IS Security; IS Security Threat; Threat Message; Fear Appeal; Literature Review.

Introduction

Rogers's (1975, 1983) protection motivation theory (PMT) is one of the mostly applied theories in behavioral information systems (IS) security research, a key area of the IS security field (Boss et al., 2015; Crossler et al., 2013). Recently, IS studies have reviewed PMT applications in IS research (Boss et al. 2015; Wall & Buche, 2017). However, those existing PMT review studies have mainly focused on fear and fear appeals[1], which represent just two of the fifteen components of Roger's PMT (see Figure 1). We argue that the 45 years of PMT studies in psychology can provide many more important insights on IS security research. The PMT insights not yet examined in IS security can help us to understand why employees do (not) comply with IS security procedures. For example, psychology literature found that appeals aimed at arousing not only fear but also empathy enhance threat message effectiveness in case that others are threatened along with the targeted individual (Haley et al., 2011; Shelton & Rogers, 1981). Hence, messages appealing to taking the perspective of the organization might help better understand employee motivation to protect the corporate data and information. Also, the PMT insights can be used to design effective interventions to improve employees' IS security behavior.

The purpose of this paper is to introduce a number of research directions from PMT research that are not yet studied in the IS security field, albeit they could increase our understanding on IS security behavior. Examining those issues in future could improve and advance our current understanding of users' information security protection motivations and behaviors, a central topic in current IS security research (Moody et al., 2018).

In the next section, we briefly describe components of Rogers's PMT and highlight its key assumptions. Afterwards, more details on our review method are provided. Based on this, we describe past research on PMT in the IS security field and how that work has addressed the existing recommendations on PMT for IS security research. We then identify five important issues that are yet unstudied in PMT research in the IS security field. Finally, we give guidance how future IS security studies can examine each issue, providing a road map for quantitative and qualitative IS security research on PMT.

Rogers's Model of Protection Motivation Theory

Components of PMT

PMT was initially designed as a special case of expectancy-value theories to better understand the relationship of fear appeals to attitude change (Rogers, 1975). Fear appeals are persuasive communications depicting a threat, i.e., unfavorable consequences that might result from not taking a communicator's recommendations (Rogers, 1975). Later, this position (Rogers 1975) evolved as Rogers (1983) moved beyond fear appeals and extended the initial PMT formulation to theorize about the effects of threatening information on attitude and behavior change (Rogers, 1983, p. 167; Rogers & Prentice-Dunn, 1997, p. 114). These revised versions (Rogers, 1983; Rogers & Prentice-Dunn, 1997) as depicted in Figure 1 received the most attention by PMT scholars and are the focus of this review.

Insert Figure 1 About Here

At PMT's core are two cognitive appraisal processes that mediate the effects of threatening information on various coping modes (Rogers, 1983). Sources of information about threats are differentiated between environmental and

intrapersonal (Rogers, 1983). The former includes verbal persuasion (in particular, fear appeals) and observational learning, i.e., observing what occurs to other people. The latter includes individual personality variables, i.e., dispositional characteristics, as well as prior experiences with similar threats, such as feedback from prior coping responses (ibid.).

If a threat is recognized, any of those sources of information can initiate threat appraisal and coping appraisal (Rogers, 1983). The threat appraisal assesses the maladaptive response(s) defining either current risky behavior (such as chain smoking) or a risky behavior that could be adopted (such as starting to smoke). Note that more than one response is possible (ibid.). Threat appraisal factors that increase the probability of the maladaptive response(s) are intrinsic rewards (such as physical or psychological pleasure) or extrinsic rewards (such as social approval). Factors that decrease the probability of a maladaptive response are the severity of the threat and one's vulnerability, i.e., one's expectation of being exposed to the threat under the condition that no adaptive response was performed (ibid.). The emotional state of fear plays only an indirect role by affecting attitude and behavior change through threat severity appraisal (Rogers, 1983; Rogers & Prentice-Dunn, 1997).

Coping appraisal assesses adaptive responses that describe protective coping behavior recommended to minimize or avert the threat (Rogers, 1983). Coping appraisal factors that increase the probability of adaptive response are response efficacy (one's belief that the adaptive response is effective) and self-efficacy (belief about one's ability and effort to successfully perform the adaptive response). Coping appraisal factors that decrease the probability of the adaptive response are any response costs—physical or psychological expenditures of adopting the adaptive response, such as difficulty, complexity, inconvenience, or overcoming habit strength (ibid.).

Threat appraisal and coping appraisal processes arouse the motivation to protect oneself as recommended, i.e., protection motivation (Rogers, 1983). According to Rogers et al. (1983, p. 172), "protection motivation is best measured by behavioral intentions". These behavioral intentions indicate the effects of persuasion and eventuate in adaptive coping, maladaptive coping, or both (Rogers & Prentice-Dunn, 1997). Adaptive coping (such as adopting a communicator's recommendation) can either involve a direct act that requires someone to do something (such as to stop smoking) or the inhibition of an act (such as not starting to smoking) (Rogers, 1983). It can further encompass a single act, repeated acts (such as annual cancer screening), multiple acts (such as participating in sports and maintaining a healthy diet), or repeated multiple acts (ibid.). Coping modes are maladaptive if the coping activity deals with induced emotions but not directly with the threat in the external situation (Rogers & Prentice-Dunn, 1997). Examples include avoidance, denial, wishful thinking, or fatalism (ibid.). It is the nature of the threat that should produce more than one mode of coping (ibid.). Any changes in adaptive and maladaptive coping will feed back as "prior experience" and induce reappraisals of the threat and coping behaviors (Rogers & Prentice-Dunn, 1997, p. 117).

Key Assumptions of PMT

PMT is applicable to "any situation involving threat" (Rogers, 1983, p. 172), including health threats, but also intra- and inter-personal threats (such as self-esteem and social relations), economic threats (such as higher energy prices), threats to other people, and even to other species (Rogers & Prentice-Dunn, 1997). However, the predictive strength of the factors varies with the threat (Floyd et al., 2000). The crucial assumption is that individuals must feel a minimum level of threat or concern before they evaluate whether they can play an effective role in minimizing the threat (Floyd et al., 2000, p. 409). Thus, PMT assumes that "motivation must be supplied first to initiate the coping [appraisal] process." (Rogers & Prentice-Dunn, 1997, p. 116).

Rogers (1983) summarizes six sufficient prerequisites to elicit this motivation and subsequent behavior to protect oneself from a potential threat. The individual must believe that 1) the threat is severe, 2) one is vulnerable to the threat, 3) the recommended protective behavior is effective in averting the threat, 4) one is able to perform the recommended protective behavior, 5) rewards from the current or potential risky behavior are compensated by factors decreasing the probability of engaging in the current or potential risky behavior, and 6) costs of the recommended protective behavior are compensated by factors increasing the probability of engaging in the recommended protective behavior (Rogers, 1983, p. 171).

Consequently, the arousal of fear is not a prerequisite to applying PMT (Rogers, 1983, pp. 169; 171). PMT usually refers to coping behaviors that are not made immediately but involve long-sustained cognitive processes (Rogers, 1983), such as taking medication or, in the context of IS security, taking IS security measures. Those kind of adaptive responses may be made after emotional states such as fear have disappeared (ibid.).

Similarly, the manipulation of fear appeals is not an essential element for PMT (Rogers & Prentice-Dunn, 1997, p. 114). Beyond changes produced by fear appeals, there are other sources of information, such as prior experiences

with similar threats that could likewise invoke motivation to initiate the threat and coping appraisal processes (ibid; cf. also Figure 1). In addition, scholars can use PMT to study not only dynamic, but also static beliefs and their impact on coping behaviors when participants perceive a threat (Rogers & Prentice-Dunn, 1997). Hypothesized effects of PMT components have been found in both experimental and correlational psychology research (ibid.). The study of Greening (1997) in health psychology is a good example of the latter without explicit fear appeal manipulations.

PMT does not assume a complete rational decision-making process (Rogers, 1983). Cognitive and motivational biases in human thinking (such as confirmation bias) are supposed to affect the threat and coping appraisal processes (Rogers & Prentice-Dunn, 1997). For instance, if people cannot perform necessary coping behaviors, increases in threat severity and/or vulnerability can induce feelings of helplessness that reinforce the maladaptive response to restore control of one's fate. This is known as the boomerang interaction effect (e.g., Maddux & Rogers, 1983).

Finally, PMT may be similar to other related theories of individual persuasion (Rogers, 1975, 1983), such as the health belief model (Rosenstock, 1974), the parallel response model (Leventhal, 1970), the cognitive-motivational-relational theory (Lazarus et al., 1970; Lazarus, 1966), and the extended parallel process model (Witte, 1992). Those theories slightly differ from each other because, while they are basically about the same beliefs, the arrangement of components and assumptions about processes are different (Floyd et al., 2000; Rogers & Prentice-Dunn, 1997; Weinstein, 1993). A comparison of those theories and their assumptions can be found elsewhere (e.g., Johnston & Warkentin, 2010; Warkentin, Johnston, Walden, et al., 2016). For reasons of scope, this review focused on those studies that explicitly measured or manipulated components of Rogers's PMT. In particular, we focused on protection motivation in response to an *IS security threat,* describing an event with potentially harmful consequences for information security (Vance et al., 2014).

Review Method

We systematically analyzed extant IS studies that applied PMT to examine responses to IS security threats. Following the approach of Webster and Watson (2002), our review process included three steps: the search process, the selection of relevant articles, and the concept-centric coding.

To ensure comprehensiveness and high quality of the source material, we searched peer-reviewed IS-centric journals as listed in Lowry et al. (2013) as well as the proceedings of leading IS conferences (ICIS, ECIS, HICSS, AMCIS, PACIS) using the search terms ("protection motivation theory" AND "information systems" AND "security") in the full text of each outlet. We then examined each article and kept those that met the following criteria: (1) the study cited PMT as the underlying theory and (2) the study analyzed an IS security threat describing an event with a potentially adverse consequence for information security[2]. In addition, we examined the references of each identified article to detect prior studies of importance and we searched forward by the means of Google Scholar to ensure we missed no relevant study citing the identified articles. This process resulted in 67 papers published in the period from 2005 to 2017. All of these studies are listed in the appendix.

We extracted from these articles scientometrics, investigated PMT components, theoretical and empirical research context, research method, PMT-related findings, and the extent to which they addressed issues psychologists discuss as important for PMT research. The Appendix Tables A.1, A.2 and A.3 provide details on our full concept-centric coding matrix as well as our coding results at length.

A Summary of Past PMT Research

Descriptive Findings

In this section, we first briefly describe the extent to which the identified previous PMT papers in IS security literature have examined each PMT component of Figure 1, which Rogers and Prentice-Dunn refer to as the "overall model of protection motivation theory" (Rogers & Prentice-Dunn, 1997, p. 114). We further summarize past methodological approaches and key empirical results.

Our systematic and comprehensive review of the 67 PMT studies in the IS security field shows that the majority (61.2% of the identified PMT articles) study other behavioral constructs or theories together with PMT in the research model. Most popular are several constructs from deterrence theory (11.9%), theory of planned behavior (10.4%), social cognitive theory (7.5%), or the health belief model (4.5%).

Regarding the PMT components (cf. Table A.1 for more details), we did not find any study testing Rogers and

Prentice-Dunn's (1997, p. 114) "overall model of protection motivation theory" as a whole (as displayed in Figure 1). The sources of information (Figure 1) have received little research attention: 22.4% of the identified studies analyzed verbal persuasion (including fear appeals), 1.5% observational learning, 1.5% personality variables, and 16.4% prior experiences with similar threats. The majority of identified PMT studies focused on the threat and coping appraisal components: self-efficacy (analyzed in 91.0% of studies), severity (89.6%), vulnerability (88.1%), and response efficacy (83.6%) were the most frequently studied PMT components. Almost half of the studies (53.7%) analyzed response costs. The investigation of intrinsic (9.0%) and extrinsic (7.5%) rewards, especially the distinction between extrinsic and intrinsic rewards, was an exception.[3] Fear was considered in 20.9% of past studies. 71.6% of the studies examined protection motivation (intention) and 56.7% the adaptive coping behaviors. These security-related protective behaviors have been examined in work environments, such as organizational insiders' volitional protection of organizational information and IS (Posey et al., 2015) and compliance with IS security policies (e.g., Bélanger et al., 2017). The behaviors have also been examined in non-work environments, such as protection against online security attacks (Chen & Zahedi, 2016), the adoption of specific anti-spyware and anti-malware software (e.g., Liang & Xue, 2010), and its continued usage (Warkentin, Johnston, Shropshire, et al., 2016). Furthermore, the security-related protective behaviors often subsume a wide range of single, multiple, specific or general security-related acts, among those 3.0% that study the inhibition of action (i.e., not to start behaving insecurely). Only 6.0% of past PMT studies investigated maladaptive coping.

Regarding the research methods used to study PMT (cf. Table A.2 for more details), 76.1% of studies tested their model with a one-time point survey. Such studies have tested the PMT, or its components, as a theory of behavior (and not as a theory of behavior change) because they have not captured change. Behavioral change settings, such as lab experiments (10.4%), field experiments (3.0%), scenario-based manipulations (3.0%), or longitudinal (4.5%) designs, are less used to examine PMT in IS security.

61 of the 67 identified articles are empirical studies. Most of these empirical studies found support or partial support for the PMT-based hypotheses in the IS security context (see Table 1). We most often identified findings in contradiction to PMT concerning the direction of the relationship between vulnerability of the IS security threat and protection motivation, which was significantly negative in 5 studies (7.5%) (Boss et al., 2015; e.g., Crossler et al., 2014; Dang-Pham & Pittayachawan, 2015).

Insert Table 1 About Here

Existing PMT Recommendations in IS Security

We found two existing reviews with future PMT recommendations for IS security. First, based on a review of 29 identified PMT-based IS security journal articles, Boss et al. (2015) recommend future IS security scholars to 1) use and establish the full PMT nomology before adding non-PMT constructs, 2) use fear-appeal manipulations, 3) measure fear, and 4) model and measure behaviors, not only intentions (Boss et al., 2015). Second, corroborating the fear-related recommendations of Boss et al. (2015), Wall and Buche (2017) propose future research questions surrounding the reactions to and effects of security-related fear appeals from a critical realist and critical constructivist stance. The existing recommendations regarding PMT thus focus on fear.

However, although Rogers originally designed PMT to understand the relationship between fear appeals and attitude change, this position evolved as he shifted his focus from "fear" to "threats" (Rogers, 1975, 1983; Rogers & Prentice-Dunn, 1997). Ever since, PMT has been applicable to "any situation involving threat" (Rogers, 1983, p. 172) and a variety of past PMT studies in psychology shows that fear appeals are not a prerequisite for PMT (e.g., Ruiter, Kessels, Peters, & Kok, 2014; Tesson et al., 2016). In existing IS security research, 22.4% of the identified PMT studies have used fear-appeal manipulations. The remaining 77.6% did not explicitly manipulate fear appeals. Previous manipulations of IS security fear appeals take one of two forms. The first form is an IS security threat message with statements that describe the IS security threat and potential benefits of practicing the recommended coping behavior (e.g., Anderson & Agarwal, 2010; Boss et al., 2015; Johnston & Warkentin, 2010; Vance et al., 2014). The second form is a hands-on training program informing the subject about the IS security threat, benefits, and secure practices (e.g., Meso et al., 2013; Putri & Hovav, 2014). Our review further identified 20.9% of the studies measuring fear arousal and its influence on individuals' protection motivation when confronted with IS security threats. The results of self-reported fear arousal measurements are mixed: some report support (e.g., Chen & Zahedi, 2016), some partial support (e.g., Boss et al., 2015), others no support (e.g., Burns et al., 2017). Self-reports might be appropriate to measure individual levels of fear perceptions. However, it is not always clear to what

extent the previously employed tools actually measure fear. To give a concrete example, survey statements such as “My computer has a serious malware problem” or “My computer might become unusable due to malware” (Boss et al., 2015, p. A10) may rather reflect malware vulnerability or concern about malware's adverse consequences rather than true fear. The only work that has applied neuroscientific fRMI methods found that exposure to IS security threat messages does not evoke fear in individuals (Warkentin, Johnston, Walden, et al., 2016). Warkentin et al. (2016, p. 205) conclude that “fear appeal theory…is not as readily applicable to addressing threats to, for example, one’s identity, hard drive crashes, or malware.”

Inspired by the history of PMT research in psychology, we propose in Section 3 (recommendations #3d and #4) alternative mechanisms that could be more relevant to influence protection motivation in the case of IS security threats than fear. After all, PMT is not intended to frighten someone but to influence one’s behavior (Tanner et al., 1989). Presently, let us highlight that the existing recommendations to study fear appeals may be relevant, but neither necessary for nor limited to studying PMT in future IS security research. Moreover, our results describing the frequencies to which past IS security studies used the PMT and non-PMT constructs (see the preceding section) illustrate that the identified IS security articles on PMT have already adopted and widely studied the non-fear-related recommendations of Boss et al. (2015).

We therefore suggest that the almost 45-year history of PMT research in psychology can inspire us with further new and important ideas that can help advance IS security research on PMT and thus, understand why employees do (not) comply with IS security procedures. We propose five broad categories of important PMT issues which past PMT-based IS security literature has not considered or not considered sufficiently. In the next section, we discuss each issue and explain its importance and relevance for behavioral IS security.

Unstudied Issues and Opportunities for PMT Research in the IS Security Field

A key assumption of PMT is that individuals must perceive a minimum level of threat for which there is an effective individual response (Floyd et al., 2000, p. 409). But what is an IS security threat, exactly? Furthermore, do individuals perceive coping responses to IS security threats as effective?

Recommendation #1: Measure the Level of Concern about IS Security Threats.

A minimum level of concern is crucial to make individuals to evaluate the coping response and in turn elicit protection motivation (Rogers & Prentice-Dunn, 1997). Concern is one’s “disposition to desire occurrence or nonoccurrence of a given kind of situation” (Frijda, 1986, p. 335). Regarding PMT, concern refers to an individual’s disposition to occupy her-/himself with cognitive appraisal of threatening information (Floyd et al., 2000).

However, IS security threats may not be like typical PMT threats that cause “pain and suffering” (Rogers & Prentice-Dunn, 1997, p. 113) or are deemed as “real but controllable threats” (Beck & Frankel, 1981, p. 204). IS security threats are digital in nature, making them intangible and invisible. They are also still relatively new and perhaps less familiar compared to health threats such as smoking or cancer. The potential negative outcomes associated with IS security threats may therefore be more difficult to grasp and anticipate. Prior studies especially conducted in work environments found that often users do not appraise IS security threats as causing them real levels of concern (Johnston et al., 2019).

We therefore suggest that researchers should not assume that subjects experience the IS security threat as concerning but should confirm experiences with research. Measuring subjects’ level of concern with the IS security threat appeared relevant for empirically supporting PMT-based models. For instance, Anderson and Agarwal (2010) measured participants’ concern regarding security threats by hackers on a 5-point scale ranging from ‘not at all’ to ‘very concerned' and found empirical support for the relevance of PMT to broader intentions to protect the Internet and the private home computer from an attack by hackers. Vance et al. (2014) found a strong prediction of security warning disregard only after the simulation of a hacker screen eliciting participants to report a significantly higher degree of concern compared to the neutral response of 5 on a scale of 0—‘not concerned at all’—to 10—‘100% concerned’. We recommend below several new approaches how IS security threat messages might be manipulated to cause users to perceive some levels of concerns through the means of personalization (recommendation #3). For now, we recommend that future studies should measure and control for a subject’s actual level of concern about IS security threats.

Recommendation #2: Measure Confidence in Relationship Between Protective Behavior and IS Security Threat Reduction.

The digital nature of IS security threats may also affect the coping appraisal. To perform protective information security behaviors, individuals may have to use technologies, such as encryption technologies or anti-malware software. Such a digital or technological mediation, which is often unobservable and intangible, may make it more difficult for people to affirm the efficacy of the recommended protective behavior.

However, a high level of assurance that the protective behavior is effective in reducing individuals' threat vulnerability significantly increases the intention to adopt this behavior (Mewborn & Rogers, 1979). In particular, if an individual's coping actions require external mediation, people must perceive a transparent contingency between protection behavior and risk reduction (Shelton & Rogers, 1981). This transparent contingency can be improved, especially for repeated protective behaviors, if people are able to monitor the effectiveness of the coping response (Beck & Frankel, 1981). An analog example for such a transparent contingency, or its lack thereof, is the "gulf of execution and evaluation" (Norman, 1988) in design research. Norman (1988) emphasizes that systems need to be designed in a way to enable both doing something (execution) and checking (evaluation) such that goal-driven users are able to derive whether their actions have moved them closer to their goals.

IS users, however, may not easily perform contingency tests to demonstrate for themselves the relationship between protective behavior and their goal of IS security threat reduction. Technically successful IS security breaches may strive to stay invisible to victims. Thus, IS users may not even perceive any immediate difference in the outcome, whether they protect their computers or not. Moreover, many users may not understand the functioning and algorithms of complex protection systems. Zahedi et al. (2015) found that displaying a detector tool's run time speed and accuracy can influence users' belief about the effectiveness of the tool in detecting fake websites (i.e., detector response efficacy). In turn, users' detection tool usage increases. Still, users are not able to retrace but need to trust in the displayed success rate when assessing the tool's efficacy to detect the threat.

Therefore, it is important to measure the level of confidence individuals have in the protective abilities of the technology and/or the organization. In the end, users must believe that their *own* response is effective and can make a difference in their vulnerability to the IS security threat (Rogers & Prentice-Dunn, 1997). The current PMT-based IS security studies do not sufficiently account for this clear contingency. For instance, most constructs of perceived efficacy are not designed to appropriately highlight the individual's contribution to facilitating the link between protective behavior and IS security threat reduction. Notable exceptions are Anderson and Agarwal (2010), who deliberately measure "perceived citizen efficacy" (with questions such as "If I adopt security measures on my home computer, I can make a difference in helping to secure the Internet"). Liang and Xue (2009) developed the technology threat avoidance theory (TTAT), which states that users who do not believe in safe-guarding measures display emotion-focused coping.

We therefore recommend that future studies should measure subjects' confidence in the relationship between protective information security behavior and IS security threat reduction.

Recommendation #3: Personalize IS Security Threat Messages.

To be persuasive, threat messages must activate theoretically relevant beliefs (Rogers & Prentice-Dunn, 1997). The relevance of a threat is distinct for each person receiving the message (Rogers & Thistlethwaite, 1970; Ruiter, Abraham, & Kok, 2001). Johnston et al. (2015) and Johnston et al. (2016) highlight the importance of personal relevance of the IS security threat. We would add that personalizing the content of threat messages and how it is expressed to targeted audiences is likewise important to enhance threat message effectiveness (Johnston et al., 2019; Tannenbaum et al., 2015; Webb et al., 2010). We propose six new manipulations to personalize IS security threat messages.

#3a) Account for audiences' threat familiarity. At first, IS researchers should tailor IS security threat message arguments to the audience's level of familiarity with the IS security threat. Familiarity with the threat and the resulting knowledge about it is identified as a critical factor that influences the level of relevance, acceptability, and accuracy at which subjects appraise the threat message arguments (De Steur et al., 2015; Higbee, 1969; Ruiter et al., 2014; Tanner et al., 1991). Two different influences have been found: First, individuals have experienced an incident that has already occurred to them or to others (Rogers, 1983). That kind of prior direct or indirect (i.e., observational learning) experiences with this or similar threats make the threat more relevant, focus individuals' attention to the response and self-efficacy information, and increase their intention to adopt the protective coping behavior (Tanner et al., 1989). Second, individuals have not experienced any incident so far but may have heard about the threat. That kind of prior knowledge moderates the influence of the threat message by affecting maladaptive coping behaviors (Tanner et al., 1991). For instance, people that have never (directly or indirectly) experienced a sexually transmitted disease (STD) although behaving risky for years by using no condom reported a higher repertory of

maladaptive responses, including statements like “I find STD-free partners” or “God will take care of me” (ibid.). When encountering threat messages, those prior maladaptive responses are reassessed and influence people’s perceptions of vulnerability and in turn the level of threat perceived (Tanner et al., 1991). Different and new arguments may therefore be necessary to convince those people (Brewer et al., 2007; Ruiter et al., 2001).

Hence, we recommend tailoring IS security threat message arguments to the subject’s current familiarity with the IS security threats. Our review shows that existing research has not yet captured participants’ (perceived or objective) threat familiarity in the design of IS security threat messages. Just eleven studies (16.4%) accounted for previously experienced IS security incidents in their PMT models. Of these, 90% reported substantial direct effects of prior experiences on the threat and coping appraisals and, in turn, on protection motivation (e.g., Tu et al., 2015). In particular, Vance et al. (2014) show that experiencing a security incident reduces security warning disregard, while users’ risk perceptions significantly increase. Mwagwabi et al. (2014) was the only study in our review evaluating any sort of observational learning (i.e., indirect experiences). They found a highly significant impact on password-related threat vulnerability if users knew someone who had ever been exposed to hacking, in addition to their own personal prior experiences.

Regarding IS security threat knowledge (but no incident experience), Anderson and Agarwal (2010), Zahedi et al. (2015), and Yang and Lee (2016) controlled for three highly significant variables: *media exposure* (“How much have you heard or read during the last year about security violations [such as threats such as virus attacks and/or unauthorized access to data by hackers]?”), *threat awareness* (“When it comes to my awareness of fake websites, I don't know anything about them/know a lot about them.”), and *security awareness* (“I know the potential security threat and its negative consequences.”). In addition, Shillair et al. (2015) found significant differences in online safety intentions between subjects with self-reported low and high levels of prior knowledge about spyware and Trojans. The drawback of these self-reporting measures is that they only capture users’ beliefs about what they know, so users who are uninformed but over-confident of their IS security knowledge may bias the threat appraisals as well as the design of the IS security threat message. Rogers and Prentice-Dunn (1997), for instance, point out that most individuals hold an *optimistic bias* and believe they are less prone to experiencing a threat than others. To overcome this bias, strong threat manipulations, especially of threat vulnerability, are necessary. Existing research has not yet studied how IS security threat messages can influence an individual's cognitive biases concerning IS security threats. Therefore, we recommend that studies should measure and test users’ actual information security knowledge, which no previous study has done so far. Such tests may help to identify cognitive biases relevant to IS security threats (cf. Tsohou et al., 2015) and to tailor messages that proactively counter previously uncovered over- and under-estimations of a subject's IS security threat knowledge.

#3b) Account for current behavior in the case of self-protection. Moreover, a subject's current risky or protective behavior determines how relevant people consider (first-time) information about a threat and the recommended protective behaviors in the threat message because this may affect the degree of threat they are currently facing (Rogers & Thistlethwaite, 1970; Ruiter et al., 2001; van ’t Riet & Ruiter, 2013). Liberman and Chaiken (1992) conducted a study revealing that non-coffee drinkers were more convinced of the link between coffee-drinking behavior and fibrocystic disease than coffee-drinking women. They concluded that the current behavior influences the impact of the threat message.

If, for instance, Johnston et al.’s (2015) fear appeal to promote the behavior of always logging off every workstation were given to two separate samples of people, those who already routinely log off before leaving their workstation and those who do not log off, we would expect different, and possibly significant, effects on the perceived threat and coping appraisals between the groups. The message might be more relevant for people who failed to log off, because they would face a higher threat that unauthorized persons had already compromised their workplace data.

We believe a connection between the IS security threat message and the participant’s current risky or protective information security behavior should help make the PMT processes in an IS security context more personally relevant. So far, this connection has not gotten much attention in IS security and most studies implicitly assume that subjects have not already adopted the coping response. We have identified only one work so far that targeted IS security threat messages to users. This work employed interactive IS security threat messages with real-time updates based on users’ current risky password behavior (Vance et al., 2013).

#3c) Account for source credibility and realism. When recipients perceive the message source as highly credible, threat message effectiveness is higher (Higbee, 1969; Pornpitakpan, 2004; Westcott et al., 2017). Although the causal relationship between smoking and health threats is complex (Thagard, 2003), by and large the general public realizes that on average, smoking increases the probability and therefore risk of getting lung cancer which, in turn, can kill you. Protection behaviors in IS security, however, are more problematic. Although those behaviors may

reduce the risk of IS security threat realization, the exact probabilities and consequences are difficult, if not impossible, to estimate (Baskerville, 1991). Further complicating the issue, phishers also use appeals to threat or security. Therefore, a message-like virus alert identifying malware with 95% certainty, which the program removes with 95% certainty (Boss et al., 2015, p. 848), may appear unrealistic or unbelievable. For instance, users, even professional ones, might ignore or avoid such messages, not because they do not believe in the IS security threat, but because they believe that such a strong link from threat to consequence is exaggerated. Doubts may arise about whether the message is due to phishing or a hoax.

Likewise, deceiving participants with fictitious IS security threats may provoke non-response due to incredibility. The large majority of 1,402 out of 1800 students (77.9%) did not respond to a fictional IS security threat appeal and did not install an anti-malware system that has no true detective abilities (Warkentin, Johnston, Shropshire, et al., 2016), but they gave us no explanation. We conclude that future studies should account for and follow up on credibility and realism of IS security threat messages, which are both unstudied issues in IS security.

#3d) Account for empathy in other protection. Often, IS security threatens others, along with the targeted individual. This is the case in both organizational and private contexts. For example, hacked personal accounts are commonly used to launch further attacks or transfer illegal material. In the case of other protection, Shelton and Rogers (1981) proposed to integrate an alternative parallel mediating process provoked by empathy, defined as "the ability to take the perspective of the other (human or infrahuman)" because "[e]mpathy bridges the gulf between the individual and the society" (ibid, p. 376). Appeals arousing empathy aim at stimulating pro-social/helping behavior, rather than persuasion. Haley et al. (2011), for instance, found that those messages appealing to the responsibility to others particularly increased women's breast-related preventative health behaviors. Accordingly, we recommend including empathy-arousing instructions in IS security threat messages because they may increase employee motivation to protect third-party IT assets, such as corporate data.

We did not find any IS security study that has taken the mediating process of empathy arousal into account. Posey et al. (2015) show that the somewhat-related concept of insiders' organizational commitment levels, defined as the extent to which an "organization's values, goals, and initiatives align with the employees' views" (Posey et al., 2015, p. 190), enhances PMT's relevance in organizational contexts.

#3e) Account for protective behaviors of prevention and detection. PMT-based studies in psychology show that people react differently to protective behaviors of prevention versus detection (e.g., Hevey et al., 2010; Leventhal & Watts, 1966). Compared to detection behaviors that are done to gather information about threat and risk factors, prevention behaviors directly reduce threat (Tannenbaum et al., 2015). While prevention behaviors generally decrease feelings of fear, detection behaviors can increase them and are therefore associated with greater perceived risk (Tannenbaum et al., 2015; Tversky & Kahneman, 1981). Prospect theory shows that people prefer risky options when confronted with losses, but prefer certainty when considering gains (Tversky & Kahneman, 1981).

Accordingly, assuming prospect theory is correct, then IS security threat messages recommending prevention behaviors are best promoted by gain frames, such as "people who change their password frequently are taking advantage of a safe and effective way to reduce compromised data." By contrast, detection behaviors that uncover IS security threats are best promoted by loss frames, such as "failing to use a virus scanner limits your ability to detect security attacks." Obtaining the unwanted and undesirable information that a virus has infected one's computer could prevail in the formation of protection motivation. Prevention behaviors, on the other hand, typically produce desirable outcomes because not performing the behavior becomes the risky option (Ruiter et al., 2001; Tannenbaum et al., 2015). For example, always logging off every workstation before walking away will bring users closer to the desired outcome of avoiding data compromise without any loss potential.

The 15 studies that manipulate IS security threat messages identified in our review have analyzed both prevention (e.g., Johnston et al., 2015) and detection information security behaviors (e.g., Zahedi et al., 2015). However, only Anderson and Agarwal (2010) accounted for prospect theory to detect the most effective mix of message characteristics that would positively affect users' home computer attitudes toward security-related behavior. The other 14 studies that reported IS security threat messages do not seem to follow any explicit theory or rule to phrase predominant losses (46.2%), predominant gains (38.5%), or a combination of losses and games (15.4%). For example, in one study, the IS security threat message frames the probable outcome solely with losses, such as "Hard drive will become unusable after the next restart; all data on this computer may be irretrievable" (Boss et al., 2015, p. 848), while the use of antivirus software after the scanning procedure, and thus a protection behavior, is analyzed. Such loss-framed information, however, can stimulate people to take more risks than usual (Tannenbaum et al., 2015), which is why such an IS security threat message could backfire.

We conclude that future IS studies should frame IS security threat messages depending on whether they examine

protective information security behaviors of prevention or detection.

#3f) Account for multiple, repeated protective information security behaviors. Frequently, protective behaviors in IS security require not only one-time single actions, but multiple and repeated efforts to be effective, such as regularly changing passwords, habitually logging off when leaving the workstation, or continuously using anti-malware systems.

Repeated protective behaviors, however, were found to be least shaped by threat messages (Tannenbaum et al., 2015). Therefore, health psychologists recommend that threat messages recommending multiple repeated actions should include specific and detailed instructions about how, when, and where actors should engage in the protective behaviors. This may prompt the motivated actors to automatically translate good intentions into actions (Ruiter et al., 2001). Automaticity is found to ensure long-term effects of threat messages on coping behaviors (Floyd et al., 2000) and can thus enhance the sustainability of the protective behavior.

In the IS security context, Vance et al. (2012) show the fundamental effect of protection habit on the threat and coping appraisal processes and subsequent intentions to comply with IS security policies. Educational training in IS security measures are found to influence the protection habit strength (Shillair & Meng, 2017). Furthermore, a higher number of IS security threat messages also tends to increase the continuance of protective behavior (Boss et al., 2015). No study so far, however, has analyzed the relevant message characteristics of one-time and/or repeated IS security threat messages that influence multiple and/or repeated protective information security behaviors over a longer period. We recommend it for future studies.

Recommendation #4: Study Maladaptive Coping with Emotions.

Coping modes are maladaptive if individuals cope with the induced emotions, but not directly with the threat in the external situation (Rogers & Prentice-Dunn, 1997). Although threatening security information appears to arouse little fear-related response (Warkentin, Johnston, Walden, et al., 2016), threatening health information is found to also arouse other emotional responses, such as surprise, puzzlement, or sadness (Dillard & Nabi, 2006; Dillard, Plotnick, & Godbold, 1996). Surprise or puzzlement in reaction to novel or abnormal IS security threat messages, or sadness in reaction to previously experienced or anticipated losses caused by an IS security breach, might be examples of potential understudied emotional responses to threatening security information.

The technology threat avoidance theory (TTAT) (Liang & Xue, 2009), which is grounded in PMT, focuses on negative emotions, such as stress or frustration. It proposes that users who perceive an IS security threat as unavoidable may mitigate negative emotions by responding with maladaptive coping. Such maladaptive coping responses can include cognitive avoidance (ignoring/trying not to think about a threat), denial (refusal to acknowledge the threat), fatalism (resigning in the face of no power to avert the threat), wishful thinking (dreaming about unrealistic solutions), or hopelessness (resignation to not being able to control the threat) (Liang & Xue, 2009; Rippetoe & Rogers, 1987).

When threatening information is personally relevant or response and self-efficacy are low, maladaptive coping responses prevail over adaptive ones (Rogers & Prentice-Dunn, 1997). Still, maladaptive coping does not necessarily suppress or counteract protective behaviors. Under certain situations, for instance, if maladaptive coping responses alleviate negative emotions, they can actually aid persuasion and boost protective motivations and behaviors (van 't Riet & Ruiter, 2013). Maladaptive coping responses can also change over time. For example, one might first deny a threat message, but then re-appraise it with increased knowledge about that threat (van 't Riet & Ruiter, 2013) (see recommendation #1). Typically, maladaptive coping is stimulated when the threat is to oneself, such as denying the threat to defend one's risky habits (Rippetoe & Rogers, 1987); when the threat is to others, individuals engage less in maladaptive coping (Shelton & Rogers, 1981).

We do not yet know the role of maladaptive coping in the organizational context when corporate IS security is threatened. Only in non-work contexts, five studies (7.5%) of our review have discussed some form of maladaptive coping. Of special note here is the study of Chen and Zahedi (2016) that finds significant positive effects, and stronger ones for Chinese than US users, of perceived online security threat on seeking help and advice, as well as on the avoidance of using the Internet to some extent, in particular for sensitive activities. Thus, the possibility of completely avoiding IS security threats by not using IT at all might be a unique attribute of IS security over other threats previously analyzed with PMT, such as health or environmental threats.

We therefore recommend future studies analyze maladaptive coping responses to emotions provoked by threatening security information in organizational contexts.

Recommendation #5: Measure Personality Variables.

As displayed in Figure 1, PMT relates personality variables to individual threat and coping appraisal (Rogers, 1983). PMT studies on health threats show that PMT predictions are more precise if, for instance, individuals' uncertainty orientation is taken into account (Brouwers & Sorrentino, 1993). Depressed and antisocial persons, as another example, are more likely to respond with maladaptive coping behaviors (Self & Rogers, 1990). And people who are highly conscious of their body appearance were found to be more motivated by messages appealing to the gains of precautionary sun behaviors than potential loss framings (Hevey et al., 2010).

In our review, Srisawang et al. (2015) is the only study that has included personality variables in PMT-based IS security models. They found that a conscientious personality positively affects threat and coping appraisals related to protective behavior against computer crime. Non-PMT-based studies in the IS security field also illustrate the importance of personality variables, such as stability, plasticity, the Big Five, or Machiavellianism for the formation of security intentions and behaviors (Johnston et al., 2016; Kajzer et al., 2014; Shropshire et al., 2015). We therefore recommend that future IS studies should start to examine individual differences in the way people process IS security threats.

Implications for Future Research

In this section, we briefly describe how future research can approach each of the five recommendations to provide a starting point. Table 2 presents a summary with example study designs and measurement items. Boss et al. (2015) suggest the use of "the core or full nomology of PMT" (Boss et al., 2015, p. 858), which means that a single study is expected to cover all components of PMT. We want to highlight that we do not have such expectations. We rather believe, consistent with PMT research in psychology (e.g., Sturges & Rogers, 1996; Wong et al., 2016) that a singular study can examine certain components of PMT. Thus, no singular study needs to cover all the issues we outlined above. In fact, a singular study can hardly study one of them in its entirety.

Insert Table 2 About Here

With respect to recommendation 1, to measure subject's actual concern about IS security threats, future research should analyze the extent to which IS security threats and accompanying IS security threat messages elicit feelings of concern. In interviews and surveys, subjects should be asked about the extent to which they feel concerned about the specific IS security threat. In variance models, ratings should either be included as control variables or those ratings below the neutral response should be excluded for analyzing PMT-based relationships. For behavior change studies, researchers should check if the IS security threat messages used are successful to elicit some level of concern in users. For this, IS security threat messages with different levels and ways of communicating the IS security threats and their negative outcomes should be designed and compared regarding their influence on users' concern regarding these IS security threats.

With respect to recommendation 2, training and tools should be designed that inform users how they can make a difference in reducing an IS security threat. Quantitative or qualitative studies can then be used to evaluate the impact of increased transparency on coping appraisal and protection motivation. In addition, the employee level of trust in protective tools, as well as in security providers, should be determined to better specify confidence in the relationship between protective behavior and IS security threat reduction.

To personalize the IS security threat message in recommendation 3, we suggest tailoring the message. In particular, people's level of familiarity with the IS security threat should be considered. Besides of people's own or observed experiences with this or similar IS security threats and their previous knowledge about them, also their currently used maladaptive behavior responses should be identified to design novel IS security threat messages that are able to change perceptions of the efficacy of those maladaptive coping behaviors. Moreover, researchers should develop tests of subjects' actual IS security knowledge. This could start with provoking and testing the performance and effects of the riskiest IS security behaviors. Next, technical IS security experts could first assess the instrument, and users should test its understandability and reliability. It is also important to provide and test translations to different languages. An alternative approach to generating such a test is to interview people and find out common, but critical, misunderstandings concerning IS security threats. It is also important to determine the extent to which people even want to know details about IS security incidents affecting them personally and, thus, how thirst for knowledge regarding IS security threats (or lack thereof) influences protection motivation. Further biases relevant for IS security threats, such as optimistic or cultural biases (see Tsohou et al., 2015), and potential counteracting interventions should be examined. To better specify the IS security threat, characteristics, and subjects' appraisal

of it, future research should also analyze how effective tools or interventions are for making digital IS security threats more visible, tangible, and known for users. Moreover, the design of the IS security threat message should consider the type of the recommended protective information security behavior (i.e., detection or prevention), and the subject's current risky or protective information security behavior. One approach for the latter is to collect self-reports on subjects' past *and* current use of risky or protective information security behaviors in a pre-study. Future research in the organizational context should also add empathy-arousing instructions in IS security threat messages to analyze the impact on employee motivation to protect corporate IT and data. Moreover, interviews are useful to follow up content credibility of IS security threat messages and determine why participants of a study did or did not perform the recommended protective behavior. It is particularly important to realize that participants who do not click a link or install an (alleged) antivirus software may do it for good reasons. For instance, they may wish to avoid an IS security threat when the recommended protective behavior is phishing-like and motivates toward a risky behavior. In addition, future research should measure the long-term effect of repeatedly recommended IS security threat messages on subjects' actual engagement in IS security measures at several points in time (i.e., at t_0, t_1, t_2, …, t_n) to derive the most effective message characteristics that provoke continued, habitual, and automatic protective information security behaviors. In particular, feedback mechanisms should be analyzed by investigating the change in participants' re-appraisal of the IS security threat and coping activity with ongoing engagement in protective behavior.

Regarding recommendation 4, to study maladaptive coping behaviors, future studies should identify alternative explanations for why protective information security behaviors are not yet adopted, even when people experience higher protection motivation. One future endeavor could analyze the extent to which subjects escape potential IS security threats by not using IT altogether (i.e., avoidance behavior) or by emotionally denying IS security threats. Here, the arousal of other emotions in reaction to IS security threat messages, such as sadness, puzzlement, or surprise, should be studied. Furthermore, it may be interesting to study how many independent types of maladaptive coping responses to IS security threats we can differentiate and how maladaptive coping changes over time. Finally, future research should investigate how maladaptive coping feeds back and affects the re-appraisal of threat and coping processes. Can we effectively encourage maladaptive responses to increase protective information security behaviors?

Concerning our last recommendation, recommendation 5, future research should analyze individual differences in the way people process IS security threat information. One example of past research into health behavior found that uncertainty-oriented persons are more motivated in situations where the coping response will resolve uncertainty about self, the environment, or any behavioral outcome (Sorrentino & Short, 1986). In the IS security context, engaging in data backups (Boss et al., 2015) or using anti-spyware (Johnston & Warkentin, 2010) or other detection tools (Zahedi et al., 2015) could help users resolve uncertainty. Thus, compared to certainty-oriented people, uncertainty-oriented people may more likely follow recommended coping responses as threat and efficacy increase and, thus, protection motivation. Future research might empirically confirm this proposition by adapting the measurement instrument for uncertainty orientation from health (Sorrentino & Short, 1986) to the IS security context.

Conclusion

We found and systematically reviewed 67 PMT studies in IS security and compared the results of this review with the application of PMT for decades in psychology. As a result, we identified several new and important issues that have not yet been examined in IS security research, and which fit into five important categories. In discussing these open issues and suggesting how future studies can approach each of them, we provide a road map for future PMT research in the IS field. It is important to note that no single study must focus on all of the issues at once.

Notes

[1] Note that fear appeals are included in the "verbal persuasion" component of Figure 1 (Rogers 1983).

[2] The selection criteria ensured a reference to the topic under study by excluding those IS studies focusing on other types of threats, such as privacy (Marett et al., 2011) or chronic diseases (Laugesen & Hassanein, 2017).

[3] Note that some studies evaluated rewards expected from the adaptive response (e.g., Siponen et al., 2009, 2010). These adaptive response rewards, though, are conceptually different from the intrinsic/extrinsic rewards expected from the maladaptive response in the threat appraisal (see Figure 1) because users evaluate adaptive response rewards in the coping appraisal to assess potential benefits from engaging in the coping behavior (Rogers, 1983).

References

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.

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. *European Journal of Information Systems*, 1(2), 121–130. https://doi.org/10.1057/ejis.1991.20

Beck, K. H., & Frankel, A. (1981). A Conceptualization of Threat Communications and Protective Health Behavior. *Social Psychology Quarterly*, 44(3), 204–217.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of Early Conformance with information security policies. *Information & Management*, in press. https://doi.org/10.1016/j.im.2017.01.003

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.

Brewer, N. T., Chapman, G. B., Gibbons, F. X., Gerrard, M., McCaul, K. D., & Weinstein, N. D. (2007). Meta-analysis of the relationship between risk perception and health behavior: The example of vaccination. *Health Psychology*, 26(2), 136–145. https://doi.org/10.1037/0278-6133.26.2.136

Brouwers, M. C., & Sorrentino, R. M. (1993). Uncertainty Orientation and Protection Motivation Theory: The Role of Individual Differences in Health Compliance. *Journal of Personality & Social Psychology*, 65(1), 102–112. https://doi.org/Article

Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68, 190–209. https://doi.org/10.1016/j.chb.2016.11.018

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

Coke, J. S., Batson, C. D., & McDavis, K. (1978). Empathic mediation of helping: A two-stage model. *Journal of Personality and Social Psychology*, 36(7), 752–766. https://doi.org/10.1037/0022-3514.36.7.752

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, 90–101.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems*, 28(1), 209–226.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. Computers and Security, 48, 281–297. https://doi.org/10.1016/j.cose.2014.11.002

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2), 285–318.

De Steur, H., Mogendi, J. B., Wesana, J., Makokha, A., & Gellynck, X. (2015). Stakeholder reactions toward iodine biofortified foods. An application of protection motivation theory. *Appetite*, 92, 295–302. https://doi.org/10.1016/j.appet.2015.05.038

Dillard, J. P., & Nabi, R. L. (2006). The Persuasive Influence of Emotion in Cancer Prevention and Detection Messages. *Journal of Communication*, 56(suppl_1), 123–139. https://doi.org/10.1111/j.1460-2466.2006.00286.x

Dillard, J., Plotnick, C., & Godbold, L. (1996). The Multiple Affective Outcomes of AIDS PSAs Fear Appeals Do More Than Scare People. Communication Research, 23(1), 44–72.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(2), 407–429). https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Frijda, N. H. (1986). The emotions. Cambridge University Press.

Greening, L. (1997). Adolescents' Cognitive Appraisals of Cigarette Smoking: An Application of the Protection Motivation Theory. *Journal of Applied Social Psychology*, 27(22), 1972–1985. https://doi.org/10.1111/j.1559-1816.1997.tb01635.x

Haley, E., Avery, E. J., & McMillan, S. J. (2011). Developing Breast Health Messages for Women in Rural Populations. *Journal of Consumer Affairs*, 45(1), 33–51. https://doi.org/10.1111/j.1745-6606.2010.01191.x

Hevey, D., Pertl, M., Thomas, K., Maher, L., Craig, A., & Ni Chuinneagain, S. (2010). Body Consciousness Moderates the Effect of Message Framing on Intentions to Use Sunscreen. *Journal of Health Psychology*, 15(4), 553–559. https://doi.org/10.1177/1359105309355335

Higbee, K. L. (1969). Fifteen years of fear arousal: Research on threat appeals: 1953-1968. *Psychological Bulletin*,

72(6), 426–444. https://doi.org/10.1037/h0028430
Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Experimental Study. *MIS Quarterly*, 34(3), 549–566.
Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. *Decision Sciences,* 50(2), 245–284. https://doi.org/10.1111/deci.12328
Johnston, A. C., Warkentin, M., Mcbride, M., & Carter, L. (2016). Dispositional and Situational Factors: Influences on Information Security Policy Violations. *European Journal of Information Systems*, 25(3), 231–251.
Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, 39(1), 113–134.
Kajzer, M., Darcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, 43, 64–76. https://doi.org/10.1016/j.cose.2014.03.003
Laugesen, J., & Hassanein, K. (2017). Adoption of personal health records by chronic disease patients: A research model and an empirical study. *Computers in Human Behavior*, 66, 256–272. https://doi.org/10.1016/j.chb.2016.09.054
Lazarus, R., Averill, J., & Opton, E. (1970). Towards a cognitive theory of emotion. In M. B. Arnold (Ed.), Feelings and Emotions. Academic Press.
Lazarus, R. S. (1966). Psychological stress and the coping process. McGraw-Hill.
Leventhal, H. (1970). Findings and Theory in the Study of Fear Communications. *Advances in Experimental Social Psychology*, 5(C), 119–186. https://doi.org/10.1016/S0065-2601(08)60091-X
Leventhal, H., & Watts, J. C. (1966). Sources of resistance to fear arousing communications on smoking and lung cancer. *Journal of Personality*, 34, 155–175.
Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71–90.
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.
Liberman, A., & Chaiken, S. (1992). Defensive Processing of Personally Relevant Health Messages. *Personality and Social Psychology Bulletin*, 18(6), 669–679. https://doi.org/10.1177/0146167292186002
Lowry, P. B., Moody, G. D., Gaskin, J., Galletta, D. F., Humphreys, S., Barlow, J. B., & Wilson, D. (2013). Evaluating Journal Quality and the Association for Information Systems (AIS) Senior Scholars' Journal Basket Via Bibliometric Measures: Do Expert Journal Assessments Add Value? *MIS Quarterly*, 37(4), 993–1012.
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. https://doi.org/10.1016/0022-1031(83)90023-9
Marett, K., McNab, a L., & Harris, R. B. (2011). Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory. *AIS Transactions on Human-Computer Interaction*, 3(3), 170–188.
Meso, P., Ding, Y., & Xu, S. (2013). Applying Protection Motivation Theory to Information Security Training for College Students. *Journal of Information Privacy and Security*, 9(1), 47–67. https://doi.org/10.1080/15536548.2013.10845672
Mewborn, C. R., & Rogers, R. W. (1979). Effects of threatening and reassuring components of fear appeals on physiological and verbal measures of emotion and attitudes. *Journal of Experimental Social Psychology*, 15(3), 242–253. https://doi.org/10.1016/0022-1031(79)90035-0
Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1).
Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. Proceedings of the 47th Hawaii International Conference on System Sciences. https://doi.org/10.1109/HICSS.2014.396
Norman, D. A. (1988). The psychology of everyday things (Vol. 5). Basic books.
Peters, L. H., O'Connor, E. J., & Rudolf, C. J. (1980). The behavioral and affective consequences of performance-relevant situational variables. *Organizational Behavior and Human Performance*, 25(1), 79–96. https://doi.org/10.1016/0030-5073(80)90026-4
Pornpitakpan, C. (2004). The Persuasiveness of Source Credibility: A Critical Review of Five Decades' Evidence. *Journal of Applied Social Psychology*, 34(2), 243–281. https://doi.org/10.1111/j.1559-1816.2004.tb02547.x
Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, 32(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Putri, F. F., & Hovav, A. (2014). Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory. Proceedings of the 22nd European Conference on Information Systems.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221–232. https://doi.org/10.1016/j.cose.2011.12.001

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, 52(3), 596–604. https://doi.org/10.1037/0022-3514.52.3.596

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 91(1), 93–114.

Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In J. T. Cacioppo & R. E. Petty (Eds.), Social Psychophysiology A Sourcebook (pp. 153–176). The Guilford Press.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection Motivation Theory. In D. S. Gochman (Ed.), Handbook of Health Behavior Research I: Personal and Social Determinants (pp. 113–132). Plenum Press.

Rogers, R. W., & Thistlethwaite, D. L. (1970). Effects of fear arousal and reassurance on attitude change. *Journal of Personality and Social Psychology*, 15(3), 227–233. https://doi.org/10.1037/h0029437

Rosenstock, I. M. (1974). Historical Origins of the Health Belief Model. Health Education & Behavior, 2(4), 328–335. https://doi.org/10.1177/109019817400200403

Ruiter, R. a C., Abraham, C., & Kok, G. (2001). Scary warnings and rational precautions: A review of the psychology of fear appeals. *Psychology and Health*, 16, 613–630. https://doi.org/10.1080/08870440108405863

Ruiter, R., Kessels, L. T. E., Peters, G.-J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, 49(2), 63–70. https://doi.org/10.1002/ijop.12042

Self, C. A., & Rogers, R. W. (1990). Coping with threats to health: Effects of persuasive appeals on depressed, normal, and antisocial personalities. *Journal of Behavioral Medicine*, 13(4), 343–357. https://doi.org/10.1007/BF00844883

Shelton, M. Lou, & Rogers, R. W. (1981). Fear-arousing and empathy-arousing appeals to help: The pathos of persuasion. *Journal of Applied Social Psychology*, 11(4), 366–378. https://doi.org/10.1111/j.1559-1816.1981.tb00829.x

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Shillair, R., & Meng, J. (2017). Multiple sources for security: The influence of source networks on coping self- efficacy and protection behavior habits in online safety. Proceedings of the 50th Hawaii International Conference on System Sciences.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion: Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, 52(12), 145–147. https://doi.org/10.1145/1610252.1610289

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Comliance with Information Security Policies: An Empirical Investigation. *Computer*, 43(2), 64–71.

Sorrentino, R. M., & Short, J.-A. C. (1986). Uncertainty orientation, motivation, and cognition. In Handbook of motivation and cognition: Foundations of social behavior Vol. 1 (pp. 379–403).

Srisawang, S., Thongmak, M., & Ngarmyarn, A. (2015). Factors Affecting Computer Crime Protection Behaviour. Proceedings of the 19th Pacific Asia Conference on Information Systems.

Sturges, J. W., & Rogers, R. W. (1996). Preventive health psychology from a developmental perspective: An extension of protection motivation theory. *Health Psychology*, 15(3), 158–166. http://dx.doi.org/10.1037/0278-6133.15.3.158

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to Fear: A Meta-Analysis of Fear Appeal Effectiveness and Theories. *Psychological Bulletin*, 141(6), 1178–1204. https://doi.org/10.1037/a0039729

Tanner, J. F., Day, E., & Crask, M. R. (1989). Protection motivation theory: An extension of fear appeals theory in communication. *Journal of Business Research*, 19(4), 267–276.

Tanner, J. F., Hunt, J. B., & Eppright, D. R. (1991). The protection motivation model: A normative model of fear appeals. *Journal of Marketing*, 55(3), 36–45.

Tesson, S., Richards, I., Porter, D., Phillips, K.-A., Rankin, N., Musiello, T., Marven, M., & Butow, P. (2016). Women's preferences for contralateral prophylactic mastectomy: An investigation using protection motivation theory. *Patient Education and Counseling*, 99(5), 814–822. http://dx.doi.org/10.1016/j.pec.2015.11.012

Thagard, P. (2003). Pathways to Biomedical Discovery. *Philosophy of Science*, 70(2), 235–254. https://doi.org/10.1086/375465

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and Security*, 52, 128–141. https://doi.org/10.1016/j.cose.2015.04.006

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information and Management,* 52(4), 506–517. https://doi.org/10.1016/j.im.2015.03.002

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, 211(4481), 453–458. https://doi.org/10.1126/science.7455683

van 't Riet, J., & Ruiter, R. A. C. (2013). Defensive reactions to health-promoting information: An overview and implications for future research. *Health Psychology Review*, 7(sup1), 104–136. https://doi.org/10.1080/17437199.2011.606782

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). *Journal of the Association for Information Systems*, 15(Special Issue), 679–722.

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013). Enhancing password security through interactive fear appeals: A web-based field experiment. Proceedings of the 46th Hawaii International Conference on System Sciences. https://doi.org/10.1109/HICSS.2013.196

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.

Wall, J. D., & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, 41, 277–300.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 92, 25–35. http://dx.doi.org/10.1016/j.dss.2016.09.013

Warkentin, M., Johnston, A. C., Walden, E. A., & Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Exploration. *Journal of the Association for Information Systems*, 17(3), 194–215.

Webb, T. L., Sniehotta, F. F., & Michie, S. (2010). Using theories of behaviour change to inform interventions for addictive behaviours. Addiction, 105(11), 1879–1892. https://doi.org/10.1111/j.1360-0443.2010.03028.x

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), xiii–xxiii.

Weinstein, N. (1993). Testing four competing theories of health-protective behavior. *Health Psychology*, 12(4), 324–333.

Westcott, R., Ronan, K., Bambrick, H., & Taylor, M. (2017). Expanding protection motivation theory: Investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC Psychology*, 5(1). https://doi.org/10.1186/s40359-017-0182-3

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59, 329–349.

Wong, T., Gaston, A., DeJesus, S., & Prapavessis, H. (2016). The utility of a protection motivation theory framework for understanding sedentary behavior. *Health Psychology and Behavioral Medicine*, 4(1), 29–48. https://doi.org/10.1080/21642850.2015.1128333

Yang, C. G., & Lee, H. J. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers*, 18, 253–263. https://doi.org/10.1007/s10796-015-9594-x

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-Website Detection Tools: Identifying Elements that Promote Individuals ' Use and Enhance Their Performance. *Journal of the Association for Information Systems*, 16(6), 448–484.

About the Authors

Steffi Haag is an Assistant Professor of Information Systems at the Friedrich-Alexander University Erlangen-Nürnberg (FAU), Germany. Her research focuses on the use and the value of shadow IT, behavioral IS security, and digital innovation. Her research has been published in Information & Management, Business Information Systems Engineering, Communications of the AIS, the Journal of Business Economics, and in the proceedings of leading IS conferences, such as the International Conference on Information Systems.

Mikko Siponen is a full professor of information systems. His degrees include doctor of Social Sciences, majoring in Applied Philosophy; MSc in Software Engineering; Lic. Phil. in information systems; and Phd in Information Systems. He has undertaken several managerial positions, including Vice dean for research (University of Jyvaskyla), Head of department (University of Jyvaskyla), Vice Head of research (University of Oulu), and director of an IS security research centre (University of Oulu). He has received over €10 million of research funding from corporations and numerous other funding bodies. His research interests include IS security, philosophy of science, cyber-crimes, and IT ethics.

Fufan Liu is a PhD student at the Faculty of Information Technology in University of Jyväskylä. His research interests lie mostly in security communication. Specifically, the familiarity, understanding and belief of persuasive messages, with their relations to individual risk perception and new forms of communication design. Complementarily, he is also interested in the genealogy and philosophy of generalized security management.

Appendix

The Tables A.1-A.3. outline the full concept matrices with details on our review results and references.

Table A.1. PMT Components Used

Reference	Components of protection motivation theory (PMT)															
	Sources of information				Cognitive mediating processes									Coping modes		
					Threat appraisal					Coping appraisal				Adaptive Coping		
	Verbal persuasion (fear appeal)	Observational learning	Personality variables	Prior experience	Severity	Vulnerability	Fear	Intrinsic rewards	Extrinsic rewards	Response efficacy	Self-efficacy	Response costs	Protection Motivation (Intention)	Single, multiple, or repeated acts	Inhibition of action	Maladaptive coping
Anderson and Agarwal (2010)	X			X	X					X	X		X			
Anwar et al. (2017)					X	X				X	X	X		X	X	
Bélanger et al. (2017)	X				X	X					X		X	X		
Boss et al. (2015)	X				X	X	X			X	X	X	X	X		
Burns et al. (2015)					X	X	X	X		X	X	X		X		
Burns et al. (2017)					X	X	X	X		X	X	X	X	X		
Chen and Zahedi (2016)					X	X	V			X	X			X		X
Chen et al. (2017)				X									X	X		
Chenoweth et al. (2009)					X	X	X			X	X	X	X			X
Chou and Chou (2016)					X	X				X	X	X	X			
Crossler (2010)					X	X				X	X	X		X		
Crossler et al. (2014)					X	X				X	X	X	X	X		
Crossler and Bélanger (2014)					X	X				X	X	X		X		
Dang-Pham and Pittayachawan (2015)					X	X		X		X	X	X	X			
Foth et al. (2012)					X	X				V			X			

Reference	Components of protection motivation theory (PMT)															
	Sources of information				Cognitive mediating processes									Coping modes		
					Threat appraisal					Coping appraisal			Protection Motivation (Intention)	Adaptive Coping		Maladaptive coping
	Verbal persuasion (fear appeal)	Observational learning	Personality variables	Prior experience	Severity	Vulnerability	Fear	Intrinsic rewards	Extrinsic rewards	Response efficacy	Self-efficacy	Response costs		Single, multiple, or repeated acts	Inhibition of action	
Garrison et al. (2016)						X										
Gurung et al. (2009)					X	X				X	X	X		X		
Herath and Rao (2009)					X	X				X	X	X	X			
Herath et al. (2014)					X					V	X		X			
Ifinedo (2012)					X	X				X	X	X				
Jenkins et al. (2013)	X				X	X				X	X			X		
Johnston and Warkentin (2010)	X				X	X				X	X		X			
Johnston et al. (2015)	X				X	X				X	X		X			
Lai et al. (2012)										X	X			X		
LaRose et al. (2008)					X	X				X	X	X	X			
Lee (2011)					X	X				X	X	X	X	X		
Lee and Larsen (2009)					X	X				X	X	X	X	X		
Lee et al. (2008)				X	X	X				X	X		X			
Liang and Xue (2009)					X	X	V			X	X	X	X	X		x
Liang and Xue (2010)					X	X	V			X	X	X	X	X		
Mani et al. (2015)				X	X	X				X	X	X	X	V		
Meso et al. (2013)	x				X	X				X	X	X	X			
Milne et al. (2009)						X	V				X			X		x

Reference	Components of protection motivation theory (PMT)															
	Sources of information				Cognitive mediating processes									Coping modes		
					Threat appraisal					Coping appraisal			Protection Motivation (Intention)	Adaptive Coping		Maladaptive coping
	Verbal persuasion (fear appeal)	Observational learning	Personality variables	Prior experience	Severity	Vulnerability	Fear	Intrinsic rewards	Extrinsic rewards	Response efficacy	Self-efficacy	Response costs		Single, multiple, or repeated acts	Inhibition of action	
Mwagwabi et al. (2014)	X	X		X	X	X				X	X	X	X			
Ngugi and Kamis (2013)						X				X	X	X	X			
Pham et al. (2017)					X						X	X		X		
Pahnila et al. (2007a)					X						X		X	X		
Pahnila et al. (2007b)					X					X	X		X	X		
Pahnila et al. (2013)					X	X				X	X		X	X		
Posey et al. (2013)					x						x			x	x	
Posey et al. (2014)					X	X		X		X	X	X				
Posey et al. (2015)					X	X	X	X	X	X	X	X	X	X		
Putri and Hovav (2014)					X	X				X	X	X	X			
Shillair and Meng (2017)											X			X		
Shillair et al. (2015)	X									X	X		X			
Sikolia et al. (2016)					X	X				X	X		X			
Siponen et al. (2007)					X					X	X		X	X		
Siponen et al. (2009)					X	X				X	X		X	X		
Siponen et al. (2010)					X					X	X		X	X		

Reference	Components of protection motivation theory (PMT)															
	Sources of information				Cognitive mediating processes									Coping modes		
					Threat appraisal					Coping appraisal			Protection Motivation (Intention)	Adaptive Coping		Maladaptive coping
	Verbal persuasion (fear appeal)	Observational learning	Personality variables	Prior experience	Severity	Vulnerability	Fear	Intrinsic rewards	Extrinsic rewards	Response efficacy	Self-efficacy	Response costs		Single, multiple, or repeated acts	Inhibition of action	
Siponen et al. (2014)					X	X		X		X	X		X	X		
Srisawang et al. (2015)			X	X	X						X		X	X		
Tsai et al. (2016)				X	X	X				X	X	X	X			
Tu et al. (2015)				X	X					X	X		X			
Vance et al. (2012)					X	X			X	X	X	X	X			
Vance et al. (2013)	X			X	X	X	X			X	X	X		X		
Vance et al. (2014)	X			X	X	X	X							X		
Warkentin et al. (2016b)	X				X	X	X			X	X		X			
Warkentin et al. (2016a)	x				X	X				X	X		X	X		
Woon et al. (2005)					X	X				X	X	X	X	X		
Workman et al. (2008)	x				X	X				X	X	X		X		
Wynn et al. (2012)					X	X				X	X	X	X			
Yang and Lee (2016)					X	X				X	X		X			
Yoon and Kim (2013)					X	X				X	X		X			
Yoon et al. (2012)					X	X				X	X	X	X	X		
Zahedi et al. (2015)	X			X	X	X				X	X		X			

Reference	Components of protection motivation theory (PMT)															
	Sources of information				Cognitive mediating processes									Coping modes		
					Threat appraisal					Coping appraisal				Adaptive Coping		
	Verbal persuasion (fear appeal)	Observational learning	Personality variables	Prior experience	Severity	Vulnerability	Fear	Intrinsic rewards	Extrinsic rewards	Response efficacy	Self-efficacy	Response costs	Protection Motivation (Intention)	Single, multiple, or repeated acts	Inhibition of action	Maladaptive coping
Zhang and McDowell (2009a)					X	X	X			X		X	X			
Zhang and McDowell (2009b)					X	X	X			X		X	X			

Note: "X": Study explicitly addressed concept; "V": Study implicitly addressed

Table A.2. Research Base, Context, Design, and Findings

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
Anderson and Agarwal (2010)	Study 1: PMT, public goods literature, concept of psychological ownership; Study 2: concepts of	Individual	Non-work	Study 1: conscientious cybercitizens' behavioral intentions to secure one's own computer and behavioral intentions to secure the Internet. Study 2: Most effective mix of message qualities that would have a positive effect on home computer attitude toward security-related behavior	Field survey & lab experiment	conscientious cybercitizens; Study1: multiple subpopulations; Study 2: undergraduate students		PLS-SEM, ANOVA	Definitive support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
	goal framing and self-view								
Anwar et al. (2017)	PMT, Health belief model	Individual	Non-work	Role of gender in cybersecurity behaviors and beliefs	Cross-sectional survey	481 employees of diverse organizations		Series of biserial point correlations	n.a.
Bélanger et al. (2017)	TPB, IS Sec literature (incl. PMT)	Individual	Work	Determinants of early conformance toward technology-enforced security policies	Cross-sectional survey after policy change	535 students, faculty, admins from a university that implemented new password policies	Yes	PLS-SEM	Partial support
Boss et al. (2015)	PMT	Individual	Non-work	Study 1: longitudinal study that used the main constructs of PMT in context of data backups Study 2: anti-malware software use in a short-term cross-sectional experimental survey	PMT review & longitudinal experiment & cross-sectional field experiment	Study1: MBA students; Study 2: undergraduate students	Yes	PLS & subgroup analysis with SEM	Study 1&2: Definitive support for high fear appeal manipulation; Partial support and contradiction for low fear appeal manipulation
Burns et al. (2015)	PMT, General Deterrence Theory (GDT)	Organization	Work	Operationalizing organizational information security as a complex adaptive system (CAS) to model the complexity of IS security risks and organizational responses using agent-	Agent-based modeling in Complex Adaptive	n.a.	Yes	Sensitivity analysis	n.a.

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
				based modeling (ABM): 1 simple probabilistic model of phishing & 2 complex theoretical models simulating the organizational security outcomes based on GDT and PMT; Sensitivity analysis of the impact of SETA training on PMT model components	System (CAS) simulation				
Burns et al. (2017)	PMT; Psychological capital	Individual	Work	Assessment of the relationship of insiders' psychological capital (PsyCap) with the mechanisms of PMT	Cross-sectional survey	377 organizational insiders		CB-SEM	Partial support
Chen and Zahedi (2016)	PMT, TTAT, poly-contextual lense	Individual	Non-work	Motivators and moderators of individuals' online security behaviors (protection against online security attacks) in the United States and China	Cross-sectional survey	Individual Internet users: US: under/graduate studens; China: acquainated social media users		ML method	Definitive support
Chen et al. (2017)	PMT, extended parallel process model, self-control theory, routine activity theory	Individual	Non-work	Antecedents of being an Internet scam victim and how it impacts online privacy concerns and privacy protection behaviors	Cross-sectional survey	11,534 Internet users		SEM with ML method	Partial support
Chenoweth et al. (2009)	PMT	Individual	Non-work	PMT-based model of users' intentions to adopt anti-spyware software	Cross-sectional survey	204 undergraduate student computer users		CB-SEM	Partial support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
Chou and Chou (2016)	PMT	Individual	Work	Understanding teachers' information security behavioral intentions and related protection motivation & Explanation of any unexpected significant effects	Cross-sectional survey	505 n-service teachers in primary and secondary education		PLS	Partial support; Contradiction
Crossler (2010)	PMT	Individual	Non-work	PMT model to empirically test why people back up data on their personal computers	Cross-sectional survey	112 computer users		PLS-SEM	Partial support; Contradiction
Crossler et al. (2014)	PMT	Individual	Both	Factors that determine whether employees follow Bring Your Own Device (BYOD) policies	Cross-sectional survey	444 under-/graduate students & employees		PLS-SEM	Partial support; Contradiction
Crossler and Bélanger (2014)	PMT	Individual	Non-work	Empirically test of effectiveness of PMT to explain a newly developed unified security practices (USP) measure for collectively capturing several individual security practices	Cross-sectional survey	81 graduate students		PLS-SEM	Partial support; Contradiction
Dang-Pham and Pittayachawan (2015)	PMT	Individual	Both	Understanding how users' intention to perform malware avoidance behaviours changes across contexts, i.e. at home and at BYOD-enabled environment.	Cross-sectional survey	252 Australian higher education students		PLS-SEM; t-test, Bayesian test	Partial support; Contradiction
Foth et al. (2012)	Technology acceptance model (TAM), Theory of planned behavior (TPB), PMT, commitment model	Individual	Work	Analysis of factors of relevance with regard to data-protection compliance	Cross-sectional survey	557 health professionals across different positions of 26 hospitals in Germany		linear regression	Partial support
Garrison et al. (2016)	PMT, TPB	individual	Non-work	Individuals' security and privacy concerns with their intention to use mobile applications	Cross-sectional survey	381 under-/graduate students		PLS	Definitive support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
Gurung et al. (2009)	PMT	Individual	Non-work	Factors that motivate the consumers to adopt and use anti-spyware tools when they are faced with security threats.	Cross-sectional survey	232 students		factor analysis, logistic regression	Partial support
Herath and Rao (2009)	Decomposed TPB, GDT, PMT, TPB, Organisational Commitment	Individual	Work	Integrated Protection Motivation and Deterrence model of employee security compliance intentions	Cross-sectional survey	employees of various organizations		PLS-SEM	Partial support
Herath et al. (2014)	TAM, TTAT, PMT	Individual	Non-work	Factors that affect user intention to adopt an email authentication service	(Longitudinal) study of two surveys	students as average email users		PLS-SEM	Definitive support
Ifinedo (2012)	PMT, TPB	Individual	Work	Factors of employees' information systems security policy (ISSP) compliance intention	Cross-sectional field survey	124 Canadian business managers and IS professionals		PLS-SEM	Partial support; Contradiction
Jenkins et al. (2013)	Stage 1: theories of routine, cognitive load, motor movement; Stage 2: PMT, theory on salience	Individual	Non-work	How monitoring a user's keystroke behavior (i.e. keystroke dynamics) can identify password reuse & displaying just-in-time fear appeals will discourage password reuse	Lab experiment	135 IS students of US university	x	t-test	Partial support
Johnston and Warkentin (2010)	PMT, technology adoption literature	Individual	Non-work	User intentions to engage in anti-spyware use recommended in fear inducing persuasive communications	Lab experiment	university staff, faculty, students	Yes	PLS-SEM	Partial support
Johnston et al. (2015)	PMT, sanctioning rhetoric	Individual	Work	Effect of sanctioning rhetoric on individuals' intention to comply with the recommended protective strategies against data theft provided	Hypothetical scenario experiment	employees of Finnish city government	Yes	PLS-SEM incl. multigroup analysis	Partial support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
				by a fear appeal under the threat of sanctions to themselves.					
Lai et al. (2012)	TTAT	Individual	Non-work	Model to explore the factors that influence consumers to adopt various identity protection practices (=technological coping) & two types of coping behaviors (techn. & conventional coping) to fight identity theft	Cross-sectional survey	117 undergraduate students		PLS-SEM	Definitive support
LaRose et al. (2008)	PMT, Elaboration likelihood model, Social cognitive theory	Individual	Non-work	Framework to motivate safe online behavior	Cross-sectional survey & lab experiment	566 undergraduate students & 206 college students	Yes	Chi-square analyses	n.a. (not all results presented, at least Partial support)
Lee (2011)	PMT	Individual	Work	Factors affecting the adoption of anti-plagiarism software	Cross-sectional field survey	218 faculty members of US public universities		PLS-SEM	Intention: Definitive support; Action: Partial support
Lee and Larsen (2009)	PMT	Organization	Work	Factors affecting small- and medium-sized business (SMB) executives' decision to adopt anti-malware software for their organizations	Questionnaire-based field survey	239 US SME executives		PLS-SEM	Definitive support
Lee et al. (2008)	PMT, Social cognitive theory	Individual	Non-work	Model of online protection behaviour, particularly regarding the use of virus protection	Cross-sectional survey	273 college students who use the Internet		multiple regression analysis.	Partial support
Liang and Xue (2009)	Process model: Cybernetics theory, coping theory Variance model: PMT,	Individual	Non-work	Development of the technology threat avoidance theory (TTAT) to explain individual IT users' behavior of avoiding the threat of malicious information technologies by using safeguarding	Conceptual	n.a.	Yes	n.a.	

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
	health belief model, risk analysis in TTAT			measures and emotion-focused coping					
Liang and Xue (2010)	TTAT	individual	non-work	Personal computer users avoidance of IT threats by using anti-spyware software	Survey	business students		PLS-SEM	Definitive support
Mani et al. (2015)	PMT	Individual	Work	Investigation of factors that influence real estate employees' intended information security behaviour	Cross-sectional survey	105 Australian real estate business employees		PLS-SEM	Partial support
Meso et al. (2013)	PMT	Individual	Non-work	Model to study college students' influence of knowledge from lectures and hands-on experience on security behavior using protection motivation theory	Cross-sectional survey	77 college students		PLS-SEM	Partial support
Milne et al. (2009)	PMT, Social cognitive theory	Individual	Non-work	Extent to which the level of perceived threat and likelihood of threat along with online self-efficacy affect risky and protective online behaviors.	Cross-sectional survey	449 consumers		OLS regression	Partial support
Mwagwabi et al. (2014)	PMT	Individual	Non-work	How user perceptions of passwords and security threats affect intented compliance with guidelines and how these perceptions might be altered in order to improve compliance.	Cross-sectional survey	419 Internet users with at least on email account		ANOVA, SEM	Partial support
Ngugi and Kamis (2013)	PMT	Individual	Non-work	PMT-based model of the coping and threat appraisals that motivate Millennials as early technology adopters to adopt or resist biometric security for system access	Cross-sectional survey with hypothetical scenario	159 millenials		PLS-SEM	Definitive support
Pham et al. (2017)	PMT, TPB, GDT, self-determination theory	Individual, Organization	Work	Description of perspectives of information security experts/managers and end-users on the impact of risk evaluation, rewards and sanctions,	Mulitple case studies	Sixteen end-users and seven security		Qualitative narrative analysis	Definitive support (if applicable: qualitative

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
				security self-efficacy and social influences on individuals' security compliance		experts and managers			"findings clearly explained the five theoretical constructs from protection motivation theory, theory of planned behaviour and general deterrence theory in the context of behavioural security compliance")
Pahnila et al. (2007a)	PMT, GDT, Theory or reasoned action (TRA), IS Success, Triandis' Behavioral Framework, rewards	Individual	Work	Factors that explain employees' IS security policy compliance	Cross-sectional survey	240 Finnish employees of one company		factor analysis, multiple regression analysis	Partial support
Pahnila et al. (2007b)	PMT, GDT, TRA, Innovation Diffusion Theory, rewards	Individual	Work	Explanation of employees' adherence to information security policies	Cross-sectional survey	917 employees of four Finnish companies		CB-SEM	Partial support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
Pahnila et al. (2013)	PMT, information quality	Individual	Work	Test whether different factors explain/predict the information security behavior of those employees who do know the ISP and of those who do not know the ISP	Cross-sectional survey	513 employees of four Finnish companies		PLS-SEM	Partial support
Posey et al. (2013)	PMT	Individual	Work	Development of a taxonomy and theory of diversity for protection motivation behaviors (PMBs) of organizational insiders to volitionally protect organizational info and IS	Interviews	Disparate groups of organizational insiders		Multidimensional scaling (MDS), property fitting (ProFit), and cluster analyses.	n.a.
Posey et al. (2014)	PMT	Individual	Work	Examination of insiders and security experts' perceptions about security behaviors and their antecedents from a PMT-based framework	Interviews	22 insiders and 11 information security professionals of different organizations and industries in the US		Thematic coding	n.a.
Posey et al. (2015)	PMT	Individual	Work	Exploration of intrinsic and extrinsic maladaptive rewards, response costs, and fear as well as SETA frequency and orga commitment and their relationships with organizational insiders' protection motivation and previously performed protection-motivated behaviors (PMBs)	Cross-sectional survey	380 insiders from various industries and positions within the US		CB-SEM	Partial support
Putri and Hovav (2014)	PMT, reactance theory, organizational justice theory	Individual	Work	Eamination of employees' intention to comply with an organization's IS security policy in the context of BYOD	Cross-sectional survey	230 employees		PLS-SEM	Partial support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
Shillair and Meng (2017)	PMT	Individual	Non-work	(1) Sources of online safety information people rely on (2) How various combinations of sources are correlated with individuals coping self-efficacy and their protection behavior habits	Cross-sectional survey	780 Amazon Mechanical Turk users		network analysis, linear regression	
Shillair et al. (2015)	PMT, Social cognitive theory	Individual	Non-work	How a sense of user personal responsibility can add to our understanding of how to educate or train users in ways that enhance their self-confidence and eventual enactment of online safety behaviors.	Experiment	441 home Internet users	Yes	2x2x2 factorial analysis	Definitive support
Sikolia et al. (2016)	PMT, TRA, Cognitive Evaluation Theory	Individual	Work	Partial replication of (Siponen et al. 2014) to explain employees' adherence to security policies.	Cross-sectional survey	110 university employees		CB-SEM	Partial support
Siponen et al. (2007)	PMT, TRA, GDT	Individual	Work	Model that explains employees' adherence to information security policies	Cross-sectional field survey	917 employees of four Finnish companies		SEM with ML method	Definitive support
Siponen et al. (2009)	TRA, PMT	Individual	Work	Factors helpful towards employees' compliance with security policies	Cross-sectional field survey	Information security pro-fessionals from five Finnish companies		factor analysis, multiple regression analysis	Definitive support
Siponen et al. (2010)	PMT, GDT, TRA, innovation diffusion theory, and rewards	Individual	Work	Understanding of why some employees comply with their organizations' security policies and others do not	Cross-sectional field survey	917 employees of four Finnish companies		SEM with ML method	Partial support; Contradiction
Siponen et al. (2014)	PMT, TRA, Cognitive Evaluation Theory	Individual	Work	Multi-theory based model that explained employees' adherence to security policies	Cross-sectional survey	669 employees from four Finnish corporations		SEM with ML method	Partial support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
Srisawang et al. (2015)	PMT	Individual	Non-work	Investigation of factors that affect computer crime protection behavior	Cross-sectional survey	600 Thai personal computer users		PLS-SEM	Definitive support
Tsai et al. (2016)	PMT	Individual	Non-work	Drivers of online safety behaviors in the context of home computer use.	Cross-sectional survey	988 Amazon Mechanical Turk users		Hierarchical regression analysis	Partial support; Contradiction
Tu et al. (2015)	PMT, Social learning theory, Social cognitive theory	Individual	Non-work	Explaining users' intentions to employ measures to reduce or prevent damage from the loss or theft of mobile devices.	Cross-sectional survey	339 US laptop or mobile users		CB-SEM	Definitive support
Vance et al. (2012)	PMT, habit theory	Individual	Work	Influence of routinized past IS security compliance behavior on the threat appraisal and coping mechanisms theorized in PMT	Cross-sectional survey with hypothetical 5 scenarios	210 employees of a Finnish organization		PLS-SEM	Partial support
Vance et al. (2013)	Fear appeals (PMT), interactivity	Individual	Non-work	Examination of the influence of interactivity, as well as static and interactive fear appeals, on motivating users to increase the strength of their passwords.	Field experiment	354 users across65 countries	Yes	ANCOVA	Partial support
Vance et al. (2014)	PMT, TPB, habituation	Individual	Non-work	Comparison of predictive power of EEG measures to that of self-reported measures of information security risk perceptions by comparing security warning disregard as well as self-reported risk perception before and after security incident screen	Lab experiment	62 students	Yes	linear regression, paired sample t-test	Partial support
Warkentin et al. (2016b)	Fear appeal theory (inkl. PMT)	Individual	Non-work	Neural activities associated with the cognitive and affective reactions to fear appeals used for promoting secure behaviors through an experimental design involving	Within-subjects lab experiment	students		fMRi & regression analysis	Partial support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
				functional magnetic resonance imaging (fMRI)					
Warkentin et al. (2016a)	PMT	Individual	Non-work	Model for explaining an individual's continued engagement in protective security behaviors	Longitudinal experiment with one cross-sectional survey	undergraduate students	Yes	PLS-SEM	Partial support
Woon et al. (2005)	PMT	Individual	Non-work	Identification of the variables that affect the decision of home wireless network users to implement security features on their network	Cross-sectional field survey	189 home users running wireless network		logistic regression	Partial support
Workman et al. (2008)	PMT	Individual	Work	Threat control model to validate assumptions and better understand the ‘‘knowing-doing” gap	Field study with online questionnaire and direct observations	588 employees		PLS-SEM	Definitive support
Wynn et al. (2012)	PMT, health belief model, TPB	Individual	Work	Preventive Adoption Model to examine factors influencing organizational users’ adoption of preventive information security behaviors	Cross-sectional survey	256 Indian employees		PLS-SEM	Partial support
Yang and Lee (2016)	PMT, GDT	Individual	Non-work	Antecedents of HIPI (Healthcare Information Protection Intention) of HIS (Healthcare Information Systems) users	Cross-sectional survey	222 HIS users who work at university hospital in South Korea		Factor analysis	Definitive support
Yoon and Kim (2013)	PMT, TRA, moral obligation, organizational context factors	Individual	Work	Comprehensive model of computer security behaviors of individuals in the workplace	Cross-sectional survey	162 employees across multiple Korean organizations		PLS-SEM	Partial support

Reference	Theoretical Base	Unit of analysis	Research context	Theoretical and/or empirical context	Research Method				Support for or contradiction to PMT-based hypotheses
					Data collection	Participants	Dynamic behavioral change	Data analysis	
Yoon et al. (2012)	PMT, social norms, habit	Individual	Non-work	Factors that motivate college students' information security behaviors	Cross-sectional survey	202 students		PLS-SEM	Partial support
Zahedi et al. (2015)	PMT	Individual	Non-work	Theory of detection tool impact (DTI) to investigate how salient performance and cost-related elements of detection tools could influence users' perceptions of the tools and threats, efficacy in dealing with threats, and reliance on such tools	Lab experiment	865 students and staff of a large Midwestern university	Yes	ANOVA, group analysis with MLM method	Partial support
Zhang and McDowell (2009a)	PMT	Individual	Non-work	Model of password protection intentions for online users	Cross-sectional survey	182 college students of 3 southern US universities		OLS regression	Partial support
Zhang and McDowell (2009b)	PMT	Individual	Non-work	Model of password protection intentions for online users	Cross-sectional survey	182 college students of 3 southern US universities		Multiple regression analysis	Partial support

Table A.3. Whether Existing Studies Have Addressed our Five Recommendations for Future Studies

Reference	#1	#2	#3 Personalize IS security threat messages						#4	#5
	Measure level of concern about IS security threats	Measure confidence in relationship & digital threat	#3a Account for threat familarity	#3b Account for current behavior	#3c Account for credibility and realism	#3d Account for empathy	#3e Account for prevention or detection behaviors	#3f Account for multiple, repeated acts	Measure maladaptive coping with emotions	Measure personality variables
Anderson and Agarwal (2010)		X					X			

Reference	#1	#2	#3 Personalize IS security threat messages						#4	#5
	Measure level of concern about IS security threats	Measure confidence in relationship & digital threat	#3a Account for threat familarity	#3b Account for current behavior	#3c Account for credibility and realism	#3d Account for empathy	#3e Account for prevention or detection behaviors	#3f Account for multiple, repeated acts	Measure maladaptive coping with emotions	Measure personality variables
Anwar et al. (2017)										
Bélanger et al. (2017)										
Boss et al. (2015)					X					
Burns et al. (2015)										
Burns et al. (2017)										
Chen and Zahedi (2016)									X	
Chen et al. (2017)										
Chenoweth et al. (2009)									X	
Chou and Chou (2016)										
Crossler (2010)										
Crossler et al. (2014)										
Crossler and Bélanger (2014)										
Dang-Pham and Pittayachawan (2015)										
Foth et al. (2012)										
Garrison et al. (2016)										
Gurung et al. (2009)										

Reference	#1	#2	#3 Personalize IS security threat messages						#4	#5
	Measure level of concern about IS security threats	Measure confidence in relationship & digital threat	#3a Account for threat familarity	#3b Account for current behavior	#3c Account for credibility and realism	#3d Account for empathy	#3e Account for prevention or detection behaviors	#3f Account for multiple, repeated acts	Measure maladaptive coping with emotions	Measure personality variables
Herath and Rao (2009)		X								
Herath et al. (2014)										
Ifinedo (2012)										
Jenkins et al. (2013)										
Johnston and Warkentin (2010)										
Johnston et al. (2015)		V								
Lai et al. (2012)		X								
LaRose et al. (2008)										
Lee (2011)										
Lee and Larsen (2009)		V								
Lee et al. (2008)		V								
Liang and Xue (2009)		V							X	
Liang and Xue (2010)										
Mani et al. (2015)										
Meso et al. (2013)										
Milne et al. (2009)									X	
Mwagwabi et al. (2014)										
Ngugi and Kamis (2013)										

Reference	#1	#2	#3 Personalize IS security threat messages						#4	#5
	Measure level of concern about IS security threats	Measure confidence in relationship & digital threat	#3a Account for threat familarity	#3b Account for current behavior	#3c Account for credibility and realism	#3d Account for empathy	#3e Account for prevention or detection behaviors	#3f Account for multiple, repeated acts	Measure maladaptive coping with emotions	Measure personality variables
Pham et al. (2017)										
Pahnila et al. (2007a)										
Pahnila et al. (2007b)										
Pahnila et al. (2013)										
Posey et al. (2013)										
Posey et al. (2014)										
Posey et al. (2015)						V				
Putri and Hovav (2014)										
Shillair and Meng (2017)										
Shillair et al. (2015)										
Sikolia et al. (2016)		X								
Siponen et al. (2007)										
Siponen et al. (2009)										
Siponen et al. (2010)										
Siponen et al. (2014)										
Srisawang et al. (2015)										X
Tsai et al. (2016)										
Tu et al. (2015)										

Reference	#1	#2	#3 Personalize IS security threat messages						#4	#5
	Measure level of concern about IS security threats	Measure confidence in relationship & digital threat	#3a	#3b	#3c	#3d	#3e	#3f	Measure maladaptive coping with emotions	Measure personality variables
			Account for threat familarity	Account for current behavior	Account for credibility and realism	Account for empathy	Account for prevention or detection behaviors	Account for multiple, repeated acts		
Vance et al. (2012)										
Vance et al. (2013)				X	X					
Vance et al. (2014)		X			X					
Warkentin et al. (2016)					V					
Warkentin et al. (2016)										
Woon et al.(2005)										
Workman et al. (2008)			V							
Wynn et al. (2012)										
Yang and Lee (2016)										
Yoon and Kim (2013)										
Yoon et al. (2012)										
Zahedi et al. (2015)		V								
Zhang and McDowell (2009a)										
Zhang and McDowell (2009b)										

Note: “X”: Study explicitly addressed concept; “V”: Study implicitly addressed

Review References

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.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of Early Conformance with information security policies. *Information & Management*, (in press).

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.

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2015). Organizational information security as a complex adaptive system: insights from three agent-based models. *Information Systems Frontiers*, 1–16.

Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68, 190–209.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors. *Computers in Human Behavior*, 70, 291–302.

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

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. Proceedings of the 42nd Hawaii International Conference on System Sciences.

Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, 65, 334–345.

Crossler, R. E. (2010). Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. Proceedings of the 43rd Hawaii International Conference on System Sciences.

Crossler, R. E., & Belanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *The Database for Advances in Information Systems*, 45(4), 51–71.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems*, 28(1), 209–226.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers and Security*, 48, 281–297.

Foth, M., Schusterschitz, C., & Flatscher-Thöni, M. (2012). Technology acceptance as an influencing factor of hospital employees' compliance with data-protection standards in Germany. *Journal of Public Health*, 20(3), 253–268.

Garrison, G. (2016). Consumer Adoption and Use of Mobile Applications: Do Privacy and Security Concerns Matter? *Issues in Information Systems*, 17(Ii), 56–64.

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.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, 24(1), 61–84.

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.

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.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2013). Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. *Information Technology for Development,* 20(2), 196–213.

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

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, 39(1), 113–134.

Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, 52(2), 353–363.

LaRose, R., Rifon, N. J. N., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3), 71–76.
Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445–454.
Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, 50(2), 361–369.
Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177–187.
Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71–90.
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.
Mani, D., Mubarak, S., Heravi, A., & Choo, K.-K. R. (2015). Employees' intended information security behaviour in real estate organisations: A Protection Motivation perspective. Proceedings of the 21st Americas Conference on Information Systems. Puerto Rico.
Meso, P., Ding, Y., & Xu, S. (2013). Applying Protection Motivation Theory to Information Security Training for College Students. *Journal of Information Privacy and Security*, 9(1), 47–67.
Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer ' s Risky Behavior and Protection Practices. *The Journal of Consumer Affairs*, 43(3), 449–473.
Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. Proceedings of the 47th Hawaii International Conference on System Sciences. Big Island, Hawaii.
Ngugi, B., & Kamis, A. (2013). Modeling the Impact of Biometric Security on Millennials' Protection Motivation. *Journal of Organizational and End User Computing*, 25(4), 27–49.
Pahnila, S., Karjalainen, M., & Siponen, M. (2013). Information Security Behavior: Towards Multi-Stage Models. Proceedings of the 17th Pacific Asia Conference on Information Systems. Jeju Island.
Pahnila, S., Siponen, M., & Mahmood, A. (2007b). Which factors explain employees' adherence to information security policies? An empirical study. Proceedings of the 11th Pacific Asia Conference on Information Systems.
Pahnila, S., Siponen, M., Mahmood, A., Box, P. O., Oulun, F.-, & Siponen, E. M. (2007a). Employees ' Behavior towards IS Security Policy Compliance. Proceedings of the 40th Hawaii International Conference on System Sciences. Waikoloa, Big Island.
Pham, H. C., Dang-Pham, D., Brennan, L., & Richardson, J. (2017). Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems*, 21, 1–16.
Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, 32(4), 179–214.
Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity. *MIS Quarterly*, 37(4), 1189–1210.
Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information and Management*, 51(5), 551–567.
Putri, F. F., & Hovav, A. (2014). Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory. Proceedings of the 22nd European Conference on Information Systems. Tel Aviv.
Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199–207.
Shillair, R., & Meng, J. (2017). Multiple sources for security: The influence of source networks on coping self- efficacy and protection behavior habits in online safety. Proceedings of the 50th Hawaii International Conference on System Sciences. Big Island, Hawaii.
Sikolia, D., Twitchell, D., & Sagers, G. (2016). Employees ' Adherence to Information Security Policies: A Partial Replication. Proceedings of the 22nd Americas Conference on Information Systems. San Diego.
Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion: Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, 52(12), 145–147.
Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, 51(2), 217–224.
Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. IFIP International Federation for Information Processing (Vol. 232), 133–144.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Comliance with Information Security Policies: An Empirical Investigation. *Computer*, 43(2), 64–71.

Srisawang, S., Thongmak, M., & Ngarmyarn, A. (2015). Factors Affecting Computer Crime Protection Behaviour. Proceedings of the 19th Pacific Asia Conference on Information Systems. Singapore.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., J.Rifon, N., & R.Cotten, S. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59(1318885), 138–150.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information and Management*, 52(4), 506–517.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). *Journal of the Association for Information Systems*, 15(Special Issue), 679–722.

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013). Enhancing password security through interactive fear appeals: A web-based field experiment. Proceedings of the 46th Hawaii International Conference on System Sciences. Maui.

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.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 92, 25–35.

Warkentin, M., Johnston, A. C., Walden, E. A., & Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Exploration. *Journal of the Association for Information Systems*, 17(3), 194–215.

Woon, I., Tan, G.-W., & R., L. (2005). A Protection Motivation Theory Approach to Home Wireless Security. Proceedings of the 26th International Conference on Information Systems. Las Vegas, 367–380.

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. J., Karahanna, E., Williams, C. K., & Madupalli, R. (2012). Preventive Adoption of Information Security Behaviors. Proceedings of the 34th International Conference on Information Systems. Milan.

Yang, C. G., & Lee, H. J. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers*, 18, 253–263.

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, 23(4), 407–416.

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace. *Information Technology & People*, 26(4), 401–419.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-Website Detection Tools : Identifying Elements that Promote Individuals ' Use and Enhance Their Performance Fake-Website Detection Tools. *Journal of the Association for Information Systems*, 16(6), 448–484.

Zhang, L., & McDowell, W. (2009a). Modeling Online Passwords Protection Intention. Proceedings of the 15th Americas Conference on Information Systems. San Francisco.

Zhang, L., & McDowell, W. C. (2009b). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. *Journal of Internet Commerce*, 8(3/4), 180–197.

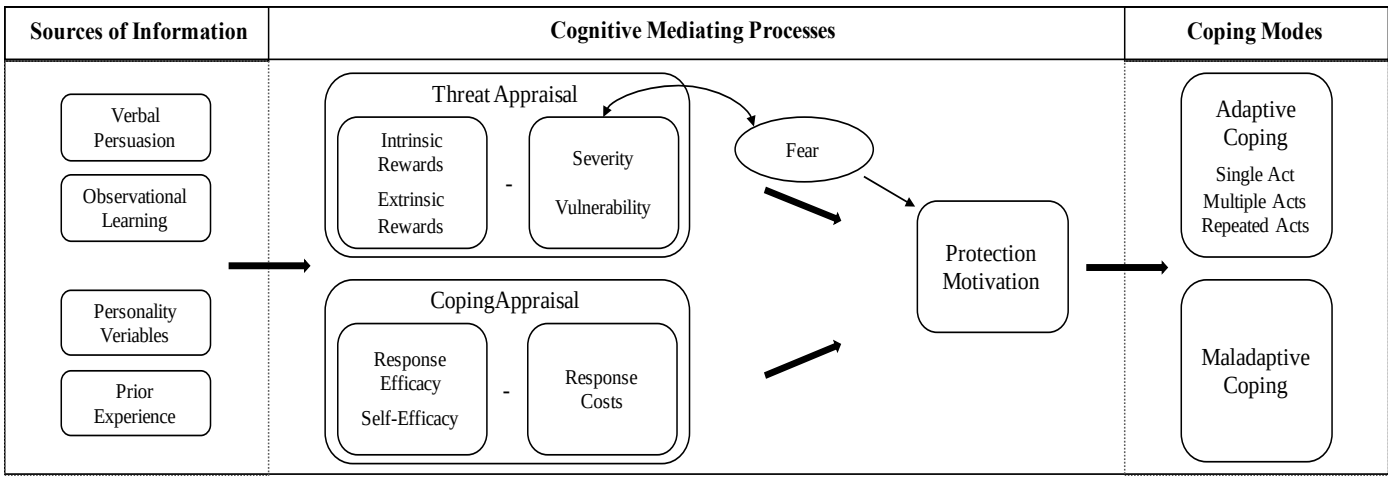

Figure 1. Model of Protection Motivation Theory (Rogers, 1983; Rogers & Prentice-Dunn, 1997)

Table 1. Empirical Results (Support, Partial Support, and Contrary Findings)

Dependent variables[e]	Definitive support for PMT[a]	Partial support for PMT[b]	Contradiction to PMT[c]	Total
Protection motivation	13 (21.3%)	34 (55.8%)	7 (11.5%)	54 (88.5%)
Adaptive coping	11 (18.0%)	23 (37.7%)	5 (8.2%)	39 (64.0%)
Maladaptive coping	2 (3.3%)	1 (1.6%)	0 (0%)	3 (4.9%)
Total	18 (29.5%)	45 (73.8%)	9 (14.8%)	61 (100%)[d]

[a] Study found support for all of its PMT-based hypotheses
[b] Study found support for some of its PMT-based hypotheses
[c] Study also found contrary results to PMT
[d] Not applicable for six of the 67 studies because these did not empirically test PMT-based hypotheses
[e] Analysis of multiple dependent variables possible

Table 2. Recommendations to Advance PMT Research in IS Security and First Examples of How to Approach Them

Recommendations of open PMT issues		Examples of how to approach the recommendations
#1	**Measure the level of actual concern about IS security threats.**	
	Analyze and control for subjects actual level of concern about IS security threats.	Examine self-reports of the extent to which people feel concerned about the specific IS security threat under study.
	Analyze the extent to which IS security threat messages elicit feelings of concern in users.	• Design IS security threat messages with different levels and ways of communicating IS security threats and their negative outcomes. • Compare which of these IS security threat messages make PMT work as theoretically specified.
	Analyze mechanisms that make the digital IS security threat more visible and tangible, and their impacts on feelings of concern, threat and coping appraisals.	• Design and evaluate tools displaying IS security attacks in real-time. • Expose subjects to a video showing how malicious offenders can misuse compromised access data and measure impact on PMT components.
#2	**Measure confidence in relationship between protective behavior and IS security threat reduction.**	
	Analyze the extent to which users are confident about/trust in the effectiveness of protective technology and protection suppliers in reducing the IS security threat.	• Interview people about their perceptions of how their protective behaviors help to reduce IS security threats. • Design tools that give feedback by visualizing a contingency between (repeated) IS security measures and IS security threat reduction (Norman, 1988). Then evaluate the impact on PMT components. • Investigate effect of self-reports about employee levels of trust in technology and their organization on PMT components.
	Analyze the extent to which users perceive that their own protective actions can make a difference in reducing the IS security threat.	• Design training interventions that educate users about how they can make a difference in reducing IS security threat. • Perform group analysis between IT and non-IT people concerning PMT components.
#3	**Personalize IS security threat messages.**	
#3a	**Account for audience's threat familiarity.**	
	Analyze the effect of users' prior direct experiences with similar IS security threats on threat and coping appraisals.	• Examine self-reports concerning the extent to which people have prior experiences with similar IS security threats. • Expose subjects to artificial IS security incidents and ask for self-reports concerning threat and coping appraisal variables and protection motivation. • Analyze differences in the effects between IS security threats individuals have previously experienced and similar threats individuals are currently facing; vary the degree of similarity between threats.
	Analyze how individuals observing IS security incidents happening to others appraise or reappraise the IS security threat.	• Expose subjects to real-world or artificial situations or to recordings showing IS security incidents happening to others and subsequently ask for self-reports concerning threat and coping appraisal variables and protection behaviors. • Examine self-reports about the extent to which people have ever observed IS security incidents happening to family, friends, or colleagues and their effects on the PMT components.
	Analyze the extent to which cognitive biases are relevant for processing IS security threats.	• Perform an analysis of variance (ANOVA) of perceptions regarding own IS security threat versus IS security threat to others to analyze optimistic bias (cf. Rhee et al., 2012). • Compare people's perceived vulnerability that the IS security threat may happen to them (such as "How likely is it that your identity will be misused if you do not engage in the IS security measure?") with the actual/statistical likelihood based on historical ID theft data.
	Analyze how subject's actual knowledge about IS security threats moderates threat and coping appraisal.	• Develop and test new instruments designed to objectively measure individuals' IS security knowledge. • Interview people about critical misunderstandings concerning IS security threats. • Determine user over-confidence effects: - Ask people how confident they are of their self-reported answers to IS

Recommendations of open PMT issues		Examples of how to approach the recommendations
		security knowledge. - Compare self-reported and objective measures of people's IS security knowledge.
	Analyze people's thirst for knowledge regarding IS security threats.	Interview subjects about the extent to which they want to know details about IS security incidents that affect them personally.
	Analyze the effect of users' prior repertory of maladaptive behaviors responses on threat and coping appraisals	• Interview people currently behaving risky about why they don't worry about IS security threats to gather relevant maladaptive responses • Analyze the relationship between the number of reported applicable maladaptive response statements and IS security threat vulnerability
	Use new, more convincing arguments in IS security threat messages for subjects familiar with the IS security threat and the recommended protective behavior.	• Capture subjects' actual knowledge about IS security threat and the recommended IS security measure(s) prior to the IS security threat message.
	Analyze interventions to overcome prevailing cognitive biases while processing IS security threats.	• Analyze the effect of disclosing/visualizing misperceptions of IS security threats on PMT components.
#3b	**Account for current behavior if self-protection.**	
	Use distinct arguments in IS security threat messages recommending protective behavior(s) for those subjects whose current behavior is risky and those subjects whose current behavior is protective	• Ask subjects prior to the IS security threat message about their past and current use of IS security measures in self-reports and/or observe it objectively. • To motivate continuance of IS security measures, highlight in the IS security threat messages what subjects have gained since using the measure.
#3c	**Account for source credibility and realism.**	
	Analyze value-based consequences of users' protective behaviors on reducing IS security threats in order to derive scientifically supported recommendations.	Assess rate of IS security incidents for users who take the IS security measure and those who do not.
#3d	**Account for empathy if other-protection.**	
	Examine the effect of a parallel empathy process in the case of protecting others from an IS security threat.	Expose employees to an IS security threat message including empathy-arousing manipulations, such as "Imagine how the reputation of your organization suffers when sensitive customer data have been lost or compromised owing to your use of easily guessed passwords. Picture how your directors, managers, or colleagues would feel. Try to be compassionate and sympathize with your organization." Let employees then complete a mood adjective checklist assessing their emotional state with empathy items such as upset, empathetic, concerned, soft-hearted, compassionate (cf. Coke et al., 1978).
#3e	**Account for protective behaviors of prevention and detection.**	
	Distinctly frame IS security threat messages recommending detection (loss frame) versus prevention (gain frame) protective behaviors.	• Gain frame in message for prevention IS security measure: "People who change their password frequently are taking advantage of a safe and effective way to keep their data secure." • Loss frame in message for detection IS security measure: "Failing to use a virus scanner limits your ability to detect security attacks."
#3f	**Account for multiple, repeated protective information security behaviors.**	
	Analyze the longitudinal effect of one-time and/or repeated IS security threat messages on multiple and/or repeated engagements in protective information security behaviors.	• Measure effect of one-time IS security threat messages on PMT components at t_1, t_2, t_3, …, t_n. • Measure effects of repeated IS security threat messages at t_1, t_2, t_3, …, t_n on PMT components at t_1, t_2, t_3, …, t_n.
	Analyze the effect of IS security threat message characteristics on habitual engagement in protective behavior(s).	Manipulate the level of specific and detailed instructions about how, when, and where IS security measures should be implemented in IS security threat messages and analyze effect on continued/habitual engagement in IS security measures.
#4	**Study maladaptive coping with emotions.**	
	Analyze emotional responses other than fear, such as frustration, stress, sadness, puzzlement, or surprise, and their impact on	• Gather and analyze self-reports about subjects' level of frustration (e.g., Peters et al., 1980), security-related stress (e.g., D'Arcy et al., 2014), sadness, puzzlement, or surprise (J. Dillard et al., 1996) in response to IS

Recommendations of open PMT issues		Examples of how to approach the recommendations
	protection motivation.	security threat messages.
	Investigate individuals' maladaptive coping with an IS security threat, esp. in organizational contexts. • Analyze the role of avoidance of IS security threats by not using specific IT, especially in the organizational context. • Analyze the role of emotional coping mechanisms, such as denial, fatalism or wishful thinking, concerning IS security threats.	• Survey subjects on: - denial (such as "I try not to think about IS security threats when using IT.") - fatalism (such as "no matter which protection I use, IS security incidents occur anyway.") - wishful thinking (such as "I wish I could use IT without any/increasing IS security threat.") • ANOVA of avoidance, denial, fatalism, and wishful thinking across varying IS security threats and/or IS security threat messages.
#5	**Measure personality variables.**	
	Analyze differences between people in processing IS security threatening information.	Examine differences in the effect of PMT components for certainty- and uncertainty-oriented people by using Sorrentino and Short's (1986) measurement instrument of uncertainty orientation.